ZONES
First Choice for IT™

Disaster Recovery Solution
WHITE PAPER

Plan for Success or Accept Failure

By Emmitt Wells, Advanced Technology Executive at Zones.

In the United States, natural disasters caused over

$1 BILLION

in damage in 2019.

Growing up on the Texas Gulf Coast, I have seen my fair share of disastrous flooding and tropical weather. My personal experience with Hurricane Harvey in 2017 still brings back vivid memories of getting households and businesses back to working order. Historically, coastlines have experienced some of the world's worst flood damage, such as the damage caused by Typhoons Lekima and Hagibis in China and Japan, which shut down business and commerce. In the United States alone, the damage caused by natural disasters in 2019 surpassed the $1 billion mark by October 10. In 2005, the damage was far worse – the total losses caused by Hurricane Katrina alone are estimated at $108 billion, making Katrina the costliest hurricane in U.S. history.

Some of these events come with an advance warning; others strike with no apparent rhyme or reason. Each can have short- and long-term effects on business continuity. The United States is exposed to earthquakes and volcanoes in the West, hurricanes across the South and Southeast, tornadoes across the Plains states, and severe snow and ice storms in the Midwest and Northeast. And these are just the most common geological events.

There are many other examples of natural disasters that put businesses worldwide at risk. Heat waves in Asia have put strain on electrical grids; wildfires in Australia have destroyed businesses and infrastructure. Already so far in 2020, earthquakes in Turkey, Cuba, and Japan have forced major consumer services offline.

Businesses can be affected by natural disasters, man-made events, and intentional attacks.

And then there are man-made disasters, which range from engineering failures to terrorist incidents such as the attacks of September 11, 2001. Consider the following categories of man-made disasters that could potentially impact your business:

- **Engineering failures**
- **Industrial disasters**
- **Mining disasters**
- **Shipwrecks**
- **Stampedes**
- **Wars**
- **Explosions**
- **Bribery and corruption**
- **Pollution**
- **Stadium disasters**
- **Transportation disasters**
- **Terrorist incidents**

And let us not forget intentional attacks. With our current COVID-19 pandemic in full swing, bad actors have more time on their hands and are launching some of the most sophisticated cyberattacks the world has ever seen. In recent months Bad Rabbit, Cerber, Dharma, Clop Ransomware, Fake Windows Update, and Zeus Gameover have caused businesses to lose a great deal of time and revenue, in some cases even forcing them to shut down.

While we cannot prepare for every possible event, we have an obligation to understand the risks that potential disasters present for our businesses, and we should all have business continuity plans ready.

Business Continuity vs. Disaster Recovery

Before we go any further, we should define two key terms in this conversation.

- **Business Continuity:** The ability of an organization to continue to function even after a disastrous event. Business continuity is the product of redundant hardware and software, fault-tolerant systems, and solid strategies for backup and recovery.
- **Disaster Recovery:** An organization's plan of action to recover in the unlikely event of a severe or catastrophic business disruption, whether natural or man-made.

Simply put, business continuity speaks to how to keep a business up and functioning if a disaster strikes, while disaster recovery speaks to the specific processes involved in resuming business. A business continuity plan takes a much broader approach to avoiding business interruptions.

A business continuity plan (BCP) is crucial for minimizing the impact of business-altering events.

5 Steps to Business Continuity Success

To help avoid business disruption, and to minimize the impact if and when disruptions do happen, it's important to have a business continuity plan (BCP). The following five elements are essential to the success of your BCP.

1. Goals and Business Impacts

Before you begin work on your BCP, it's important to first define your goals, being sure to consider feedback from other stakeholders in your organization. Businesses are built on three foundational elements , known as the "three P's"– property, personnel, and processes. Without these three elements in place, it's impossible to conduct business in a manner that keeps your employees healthy, clients happy, and company profitable. It's therefore essential to consider these elements as you define the goals of your BCP.

The initial questions to answer are very simple:

- **Do you have backing from management?**
- **What is the purpose of your business, and why is it important that it functions continuously?**

The answers to these questions should provide the foundation for your plan. With a strong foundation, you can begin the process of establishing goals, assessing risks, and defining business continuity priorities.

It is not an option to work through this process alone, isolated from the rest of the business. All relevant decision-makers must be involved, providing key insights into the process. The following are a few examples of questions you can ask that will help with defining goals and objectives:

- **What critical functions exist within the business?**
- **Who is critical to those business operations?**
- **Is your business getting oil out of the ground?**
- **Do your clients need 24/7 access to financial information?**
- **Do you lose money if your assembly lines are down?**
- **What if the lines of communication with design and implementation staff break down?**
- **What laws or regulations are on the books that will impact your plan?**
- **What should be included? Excluded?**
- **What are your security goals?**

At this point in the process, you should be collecting as much data as possible. For each identified threat, calculate the associated risk, determine the duration of impact, calculate the associated costs, and identify security concerns.

Can your business prevent a disaster before it starts?

Explore whether processes or technologies can be put in place to eliminate risk, or simply to reduce it. That is, can you insert preventative controls, or would they only lessen the impact of a potential disaster? There is no right or wrong answer to this question; your perspective will depend on your business requirements. The conclusion you reach will set the stage for the next phase in this process.

2. Controls and Strategies

In the previous step, we identified a lot of data. In this step, we begin to shape that data into information that's usable in your BCP. As part of your collection, you have controls and you have strategies. This is where a consultant or industry expert comes in handy, to help you navigate the different possible methodologies and identify the best match for your business needs.

You should spend some time familiarizing yourself with both the controls and strategies to ultimately merge the two into an effective plan. While you do not necessarily need to build the full bridge at this time, you can at least eliminate those that do not apply or cannot be implemented due to cost constraints or other business reasons.

Questions to answer in this step include the following:

- **How do your business processes interrelate, and in what order do they need to be implemented?**
- **What are your top data recovery priorities?**
- **What kind of data backup and recovery methods exist or are available?**
- **Do you need a backup facility? To what extent are you using it?**
- **What does your environment have to look like to be completely functional?**
- **Are your preventive or reduction controls as secure as your normal operations?**

During this stage, you should begin to assign incident levels. Each level brings its own set of controls and strategies.

- **Level 1:** A simple outage with an easy workaround.
- **Level 2:** A major outage where business continuity plans are needed to provide the appropriate level of service.
- **Level 3:** A disaster where a DR plan is put into full effect to bring up a backup facility or other alternative.

A Level 1 incident could be as simple as a remote connectivity failure. For example, a primary access point covering a set of cubicles could fail, and users would be redirected to a secondary unit with overlapping capabilities. In most cases, the users are not even aware that the primary system has failed. Business operates normally.

It's easy to recover from a Level 1 incident; a Level 2 or 3 incident, however, can be business-threatening.

A Level 2 incident could be much more complex. Say a tropical storm dumps a tremendous amount of rain on a facility in a coastal area. This would affect your call center, as employees would not be able to safely get in and out of the facility due to flooding. Your BCP would need to allow for calls to be rerouted to a redundant facility until normal operations could recover.

An example of a Level 3 incident would be a terrorist attack on an office building, where your entire facility was lost in a fire. Your disaster recovery plan would need to kick in, and a second site would need to be brought online, complete with systems and personnel. Downtime could be several days or several weeks, depending on the criticality of the business systems and the strength of the plan you have in place. Operations would remain in the second site until the primary facility was ready to retake operations.

Another important part of this step is to identify the resources that you will work with during the final two steps of your program. These are the employees that will be responsible for executing and continually enhancing your BCP.

Sometimes, these are the same people you are working with today, but more often than not, this process is turned over to a different group once the plan is developed. And just like getting management buy-in, these employees must be on board with what you're trying to accomplish; otherwise, you risk going through an extremely grueling effort and getting no results.

3. Plan Development

In this step, you should take the business intelligence you've gathered so far and use it to map out a clear and concise plan to move forward.

You will need to define how you'll implement your plan, when you'll put it into action, how and when to conduct proper tests, and what actions you can take to keep your plan on the minds of every individual within your organization.

You should include elements such as analyzing inputs, developing procedures, recovering documents, assigning roles and tasks, and determining success factors. Also include a list of your first response team members (including all relevant contact information), response directives, a test plan and schedule, and plans for maintenance and management.

Remember: Business continuity is about keeping the business running, no matter what the disaster. This could mean instating temporary measures until your disaster recovery plan kicks in or a permanent solution is available.

While developing your plan, it is important to define the organization's risk appetite. Three elements will determine this appetite: How quickly data must be recovered (your recovery time objective, or RTO), how much data must be recovered (your recovery point objective, or RPO), and how much the organization is willing to pay for the recovery.

How quickly do you need to recover?

Your disaster recovery plan will vary depending on your individual business needs.

Answers to this question can vary from "immediately" to "whenever." Many factors will go into this calculation. Ultimately, this is not an IT decision – only business leadership can define the impact that the prolonged loss of a given operation will have.

How much data can you lose?

Every part of the business has a certain level of tolerance for data loss. Some are higher than you may expect – for example, you could have a business process that simply relies on current information. Certainly, recovering historical data would be helpful, but losing it would not impede operations in a significant way.

What is the cost of recovery?

Once you've gathered all the facts, you next have to evaluate what processes and technology you should use to achieve your recovery goals. You may have to make tradeoffs here, as quicker recovery and lower data loss often lead to higher implementation costs. Here is where IT can play a key role. In the strategy step, you looked at many solutions; now, it's time for IT to evaluate them and determine the best course of action.

Your recovery costs will revolve around the six areas listed below. It is important to note that these may be weighed quite differently from one business unit to another.

- **Business Recovery**
- **Employee and Client Communications**
- **Facility Recovery**
- **IT Recovery**
- **Data Loss Recovery**
- **Event Escalation**

The final step in the planning process is to validate your plan against the goals you established in the first step of the process. Business leadership must validate the plan, as they are the major stakeholders in its success or failure. Your plan is not worth the paper it's printed on without their endorsement.

Rigorous testing will ensure that your DR plan is ready for use when it's needed.

4. Testing

Your testing plan is a very important aspect of your BCP. Often, organizations do a good job defining their plans initially, but they fail to test whether they still work or are even valid. Without periodic testing, how will you know your plan still works and is still applicable to your business requirements?

The key to success is testing, whether that's a simple walkthrough or a full-blown contingency test. The owner of the BCP works closely with the business to schedule and evaluate each test, so that issues can be identified and additional functionalities can be added. Tests must be fully documented so that the results can continually be referenced throughout the growth and development of the plan. At a high level, the testing involves the following activities:

- **Working with business units to test processes and procedures.**
- **Identifying those that work well.**
- **Identifying those that need improvement.**
- **Detecting any impediments to proper testing.**

There are several types of testing methodologies. The following are recommended to limit downtime and unnecessary business vulnerabilities.

- **Once a year:** Real test of business failure.
- **Once a year:** General walkthrough of processes without actual failure.

Again, do not let your test plans sit on a shelf and become just another set of processes that become obsolete. Put your plans to the test and make sure your business will still be able to continue in the face of a real disaster.

5. Maintenance and Management

Just like your test plan, your BCP must be continually reevaluated and fine-tuned as your business evolves. A good piece of advice is to retain your BCP team if at all possible. Many organizations disband their teams after a BCP is in place, but this isn't usually a good idea. Let me share a typical scenario.

A large energy chemical company wants to ensure that their point of sale devices maintain communication with their corporate offices at all times. The company gathers key people from IT and other business teams to formulate a business continuity plan that involves hard-wired connectivity.

During development, co-workers backfill the team members' everyday jobs so the team can focus on creating the plan. They assemble a great plan and then go back to their normal responsibilities. The CIO then puts a stamp in the correct box to denote that a BCP exists and that no further work or testing is necessary.

62% OF BUSINESSES

have experienced at least one phishing and/or social engineering attack within the last three years.

Several years later, the company undergoes significant change. Through acquisition, the company adds 120 retail locations that use a newer POS application, and leadership decides to use this application in all locations. The old hard-wired connectivity is no longer needed and is replaced by new wireless cell connectivity. The existing BCP does not take into account public wireless access, the newer POS system, or additional sites, and it needs to be updated.

As you can see, this company no longer has a plan that will maintain business continuity. This example goes to show the importance of maintaining an active team, so as to ensure continuous responsibility and keep the BCP valid.

If you need one more example to convince you to maintain a BCP team, consider security. Security disasters change with the ebb and flow of technology advancements. Certain attacks become more prevalent, technology improves protection, new methods of attack are developed, and so goes the continuous circle.

- We saw COVID-19-related phishing and malware attacks increase dramatically in 2020, from a few thousand per week in February to over 200,000 per week in late April. In May and June, as countries started to ease lockdowns, threat actors also stepped up their non-COVID-related activities, with a 34% increase in all types of attacks between April and June. (Check Point)
- 62% of businesses have experienced at least one phishing and/or social engineering attack within the last three years. (Cybint Solutions)
- Data breaches exposed 4.1 billion records in the first half of 2019. (RiskBased)
- The top malicious email attachment types are .doc and .dot which together account for 37%. The next most common is .exe, at 19.5%. (Symantec)
- 52% of data breaches feature hacking, 28% involve malware, and 32–33% include phishing or social engineering. (Verizon)

If you are not updating your BCP to accommodate these new threats, then what good is your plan?

Your BCP team must have the right resources and schedule availability to provide ongoing support. Also, your plan must integrate into your organization's change management process to ensure it is not compromised when other changes are made. Going off of your existing change management process is probably the easiest way to make sure your BCP is updated as your business changes.

By inserting a step called "BCP update" toward the end of your process, you will have an automatic hook into the management of your plan and a method for keeping your BCP team aware. Your team will be smarter and more effective, and your plan will be adaptable to meet ever-changing business needs.

With a good plan and frequent testing, you can provide the foundation for your business operations to continue in the face of any disaster.

In Summary

A successful business continuity strategy can be summed up in three main points:

- **Thorough requirements gathering:** Remember that the three P's (property, personnel, and processes) must each be given due consideration as you prepare your business continuity plan. Do not develop a BCP that ignores your business needs and overlooks the reasons you must continue to operate.
- **Validated plan development:** Use a methodical approach to develop your BCP. Involve both IT leaders and other business stakeholders in the process. Answer all the key questions at each stage, as each is critical to the successful implementation of your plan.
- **Ongoing management:** Regularly test, validate, and revise your plan. Remember that your plan is not a piece of artwork to be admired, but a working document that will grow and change with your business.

Other Resources:

- **Business Continuity Institute (BCI): www.thebci.org/**
- **Disaster Recovery Institute International (DRII): www.drii.org/**
- **Association of Contingency Planners (ACP): www.acp-international.com/**

About the Author

Emmitt Wells, is an Advanced Technology Executive at Zones, located in Houston. He has contributed to building and consulting on global solution sets in the areas of Network, Wireless, Voice, Data Center, and Application Management Services. He currently focuses on selling cloud-first solutions in the area of Workplace Modernization (End User Compute & Productivity, Collaboration, and Store & Branch Modernization), Network Optimization (Wired & Wireless Networking, WAN Optimization, and Network Security), Data Center Transformation (Virtualization, Storage, and Hyperconverged Infrastructure), and Security Fortification (Security Assessments, Endpoint Security, and Authentication & Data Security).

About Zones, LLC

For over 30 years, Zones has worked with industry-leading partners to offer comprehensive IT solutions to clients around the world. Our Workplace Modernization, Network Optimization, Data Center Transformation, and Security Fortification solutions lead clients through their digital transformations, and our services offer support every step of the way. That's what makes us the First Choice for IT.™

Corporate Headquarters
Zones, LLC
1102 15th Street SW, Suite 102
Auburn, WA 98001-6524