<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Why you need DR and BC</td>
<td>3</td>
</tr>
<tr>
<td>What constitutes a “Disaster”?</td>
<td>4</td>
</tr>
<tr>
<td>The difference between disaster recovery and business continuity</td>
<td>5</td>
</tr>
<tr>
<td>The hidden effects of a disaster</td>
<td>6</td>
</tr>
<tr>
<td>Steps to an effective business continuity plan</td>
<td>7</td>
</tr>
<tr>
<td>What it takes to get started</td>
<td>10</td>
</tr>
</tbody>
</table>
Chapter One

Why You Need Disaster Recovery and Business Continuity

Organizations needs to devote some thought and planning to contingencies for disaster recovery (DR) and business continuity (BC) to ensure the business can survive an unexpected interruption of business operations. Any unexpected interruption can threaten an organization, and the magnitude of the threat depends upon how well the organization is prepared for such a disruption.

Many businesses find the challenges preparing for a disaster more daunting than the risk of not being prepared. Possibly the three biggest challenges are:

- Not knowing where to begin (lack of required knowledge or experience to implement a DR/BC plan)
- Costs of DR technologies
- Lack of resources (time and/or personnel) to implement and maintain a DR/BC plan

This e-book will address these challenges, provide information, ideas and the steps to set a plan in motion to ensure that your business continues to serve its clients and provide employment for your staff.
When heads of organizations hear the word “disaster”, the images that come to mind immediately are flashing lights, screaming sirens and brave first responders – the things that are the leading stories on the evening news.

When talking about disaster recovery in a business context, a disaster can be anything that causes an interruption in business operations. This could include: fires, earthquakes and tornados, a flooded server room from a burst pipe. A crashed server won’t make the evening news, but it can halt your business operations. Even an accidentally deleted file can be a disaster.

Planning for disaster recovery should take into account a number of scenarios and determine the impact, and likelihood of each scenario.

The key is, everything has a cost and you want to spend to address the areas that are the most important for your business.

On the most dramatic end of the scale, if your entire region is disrupted to the extent that the infrastructure of society is broken down, nobody’s going to be doing business, so only a company with a statewide, national or international would need to invest to deal with disasters of that scope.

Being prepared for a crashed server, or a localized flood or anything that night render your office unusable is worthy of consideration, even for regional businesses. And technologies exist to make this recovery and (rapid resumption of business) viable.
The two terms “disaster recovery” (DC) and “business continuity” (BC) are inextricably linked, but it is important to understand the distinction.

Disaster recovery usually refers to the resumption of systems affected by a disaster. For instance, restoring lost data from a backup is disaster recovery. Typically, disaster recovery addresses specific systems at a time, and is tactical in nature.

Business continuity refers to actions taken to resume normal business operations after they interrupted by a disaster. It is both tactical and strategic in nature.

When the disaster is relatively narrow in scope (like the data loss described above), the mere act of restoring the data - recovering from the disaster – resumes operations disrupted by the disaster- so the distinction between DR and BC is not meaningful in that example.

But often disasters don’t only affect a single system, and when that happens, merely fixing the systems isn’t enough to bring the business back to normal operations. Realizing this, and planning for it, are crucial to ensuring a business does not suffer lasting consequences from disaster, big and small.

Any interruption in services that is noticeable to your client base will require communications to that client base during and after the interruption, or you risk losing client confidence in your business. The same applies to your employees and your suppliers – they all need to know what’s going on, and what’s being done, and that takes some planning.
Disasters rarely affect only one part of a business. If a business disruption lasts more than a few minutes, there are effects that you may not be aware of. These can include:

**Costs for Lost Productivity**
If your employees can’t work due to data or technology not being available for a length of time, you lose money whether you send them home for the duration or let them wait it out at work.

**Damage to Company Image and Reputation**
Your clients may tolerate a brief disruption but not for very long. They have work to do, too, and they won’t hesitate to take their business elsewhere if it appears that your company is prone to outages or unprepared to deal with them.

**Compliance and/or Regulatory Impacts**
Your industry may require you to have certain systems maintain a high availability. If you’re unable to meet those requirements, there can be fines or other penalties.

The point is, business disruptions are costly and tend to cost more than you might think and those costs mount very quickly. Moreover, the effects can last longer than the actual disruption. This information needs to taken into account when deciding what your business can afford to do to be prepared to recover operations quickly after something happens. The results of some of these disaster scenarios may well be much more costly than the price of mitigating them.
Following these steps can result in a plan that will prepare your business for scenarios for which it is reasonable to be prepared.

**Step One: Business Risk Assessment**

This is the step where you and your team brainstorm all the disaster scenarios that you can come up with. Look at various parts of your business operations and try to imagine what could happen to bring them to a halt, or render them otherwise unusable – don’t even worry about plausibility yet.

For example: What if your mail server goes down? What if you’re sabotaged by a disgruntled ex-employee? What if your power goes out? What if the office burns down? What if there’s a natural disaster?

**Step Two: Business Impact Assessment**

Now you have a list of possible (if not plausible) disasters. For each one, two determinations need to be made:

- What is the impact of the disaster?
  - Would you rate it as high, low or somewhere in the middle?

- What is the probability of the disaster?
  - Would you rate it as high, low or somewhere in the middle?

Picture a chart like the one on the right to decide whether or not each scenario needs to be seriously addressed in your Business Continuity Plan. Some companies use a 4-point scale to rate Business Impact:

1. Highly Critical
2. Critical
3. Important
4. Deferrable.

The idea is, at the end of these first two steps, you have a list of disaster scenarios that your BC Plan will be designed to mitigate.
Step Three: Disaster Recovery Plan

For each of the systems that would be interrupted by the disasters on the list, determine which measure you will take. Factors to consider are:

**Recovery Time Objective (RTO)** – this means, what is time goal for the system being restored after a disaster. Obviously, “immediately” is the ideal RTO, but you’ll have to determine what’s possible and what’s affordable.

**Recovery Point Objective (RPO)** – this means, when you utilize the DR plan, at what point in time will you need to restore too, after a disaster. Again, there’s a theoretical ideal (1 nanosecond ago), but you’ll to determine what is possible and what is affordable.

**Layers of Defense** – for some systems, it may be desirable to have some post-disaster options and these can favorably affect your RTO and RPO. For example, for a data loss, your recovery time can be very rapid if there’s a backup onsite, attached to the network. If your whole network is affected, you would also want backups to be stored offsite as well.

**Failover Mechanisms** – some DR processes can be automatic, or nearly so. If a server fails, and there’s a mirrored version on the network, the “spare” could be pressed into service very quickly. If the whole network is affected, then you would want to fail over to a virtualized environment in the cloud. Plan how these mechanisms should work and understand their capabilities and limitations.

Step Four: Implement Solutions

In addition to the technical components of your DR plan (data backup, failover, redundancies, etc.), it’s important to plan the operational response to a disaster.

It needs to be abundantly clear (and documented) who’s in charge of what when a disaster affects the business. Given the unpredictable nature of disasters, your plan has to work when some of the responsible people can’t be found. Depending on the duration of the event, it may be necessary to contact employees, clients and suppliers.

Don’t even assume your technical people will be available – therefore, the actions required to fail the business over to a virtual environment need to be understood by any of a number of principals in the company.

Vital information such as financial information, contact info, login/password info and access codes need to on lists kept up-to-date and stored at several offsite locations in a secure manner.

This is a general overview - space doesn’t permit going into to much detail in this e-book. Each of the parts of the disaster recovery plan is important, the plan is only as good as its weakest component, so careful planning and thorough execution are important for this step!
Step Five: Test the Disaster Recovery Solutions

It is a truism that in times of stress, people’s actions will revert to their training. Fancy failover systems or data restoration plan aren’t much use if no one knows they work. So, testing the DR solutions is vital.

Make sure you (and somebody else at your company) can restore data and images from both local and offsite backups. Make sure you (and somebody else at your company) can bring backup servers online, whether they’re local or virtualized in the cloud.

Try and test scenarios where your main IT people are not available and make sure the secondary and tertiary contacts can restore the vital systems within an acceptable timeframe. Professional technology management and solutions based companies such as Clare Computer Solutions provide disaster assessments and tests for various aspects of the business. These tests and assessments can often be the first time a client’s disaster recovery plan has ever been tested or reviewed by an outside source.

Remember, as there are very good reasons for having fire drills, businesses need to test their resources and systems before a disaster strikes.

Step Six: Train and Maintain

Nothing is static in business and technology, and this means your Business Continuity plan needs to be updated as personnel changes, your business changes or your technology changes.

Any time a person leaves your company that had a specific duty in your business continuity plan, that person needs to be replaced and the replacement documented – everywhere that documentation exists. Any time something new is added to what your company would consider a vital part of the business, emergency support and recovery for that system needs to be designed and documented.

Any new employee needs to be made aware of the company’s business continuity plan and trained in its details and any involvement the employee has in it.

Regular drills will ensure the right people are in the loop – if your drill fails to resume operations after a “test” disaster, it surely won’t work when you really need it! Therefore, a drill needs to be taken seriously, not a cursory walk-thru.
What it Takes to Get Started

Designing and implementing an effective business continuity plan doesn’t happen overnight. There’s a lot of thought and a lot of work that goes into it. So, how does an average company manage to do this without disrupting their day-to-day operations and diverting time and resources that are vital part of those operations?

The first thing you need is commitment. If anyone involved in the process doubts the company’s will to implement the plan, there will not be sufficient energy to see it through.

Creating a continuity plan is a major project – but it’s also the beginning of a process that will never be done. That needs to be understood and part of the commitment as well.

Like any important undertaking, break the design and implementation into steps – roughly analogous to the chapters in this brief e-book. Put key people in charge of the parts of the process, and set achievable milestones for them.

Don’t hesitate to get outside help. Very few small-to-medium size companies have business continuity experts on staff, and even fewer have “spare” personnel to devote to developing and implementing the plan. You can rent this expertise, rather than buy it.

Clare Computer Solutions has helped many companies make and disaster recovery part of a business continuity plan, and we have helped a number of companies embark on a BC plan. Since IT support is about business processes and operations, we understand the need to build disaster recovery and business continuity into the IT infrastructure and the business operation.

We’ve seen it work for these companies, and it will work for your company too. So what does it really take to get started?
It just takes a conversation with Clare Computer Solutions.

It all starts with a conversation with Clare Computer Solutions