IF DISASTER STRIKES IS YOUR BUSINESS READY?

DISASTER RECOVERY and BUSINESS CONTINUITY: WHAT YOU NEED TO KNOW
Many business owners put off disaster planning, perhaps thinking that it won’t happen to them.

Most business owners would agree that it is a smart choice to have an up-to-date Disaster Recovery and Business Continuity plan that documents the process, policies and procedures to follow in order to protect a business and its assets in the event of a disaster. A plan needs to be designed so that a business can get back up and running as quickly as possible after a disaster.

According to the Insurance Information Institute, 40 percent of SMBs that are forced to close because of a disaster will never re-open. Other studies show that between 70 and 90 percent of all businesses hit by a disaster are out of business within two years.

Don’t be a business without a current plan. Creating one will provide security and peace of mind that your business will be up and running and will survive in the event of a disaster.
Disasters Come in All Shapes and Sizes

What Are Disaster Recovery and Business Continuity Plans?

**Disaster Recovery Plan**
A Disaster Recovery Plan defines actions to take in response to a disaster with the goal of restoring the availability of specific services, systems and/or facilities that have been made unavailable by the disaster.

**Business Continuity Plan**
A Business Continuity Plan prepares a business well in advance for disasters. It is designed to ensure that following a disaster critical business functions will be available to customers, suppliers, regulators, and other entities.
Steps to an Effective Business Continuity Plan

1. Business Risk Assessment
2. Business Impact Assessment
3. Disaster Recovery Plan
4. Implement Solutions
5. Test Plan
**Steps to an Effective Business Continuity Plan**

1. **Business Risk Assessment**

   Begin preparing your plan by considering the risk to your business, employees and customers if any of the following occur:

   - No Internet connection
   - Office burns down
   - Floods destroy all office equipment
   - Massive power outage
   - Computer system sabotage
   - Important files and documents accidentally deleted
   - Terrorist attack or other global event
Steps to an Effective Business Continuity Plan

2. **Business Impact Assessment**

Identify functions that are critical to your business and the systems required to support them. Consider the impact on your employees, clients, customers, supply chain, legal requirements, loss of revenue, and the company's overall reputation if the following were not available:

- Access to files, documents
- Fulfillment system, product order inventory
- Distribution/Delivery
- Email
- Internal and external communications
- Production
- Telephone
- Medical or Financial Records
- Payroll System
# Steps to an Effective Business Continuity Plan

## Business Impact Assessment (cont.)

### Theoretical Example: Hospital

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Timeframe</th>
<th>Recovery Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HIGHLY CRITICAL</strong></td>
<td>Adverse impact to business operations.</td>
<td>Less than 12 hours</td>
<td>High availability disaster tolerance failover. Back up via SAN.</td>
</tr>
<tr>
<td><strong>CRITICAL</strong></td>
<td>Some impact to clinical care and/or patient safety. Possible adverse impact to critical govt. services.</td>
<td>1 - 24 hours</td>
<td>Traditional hotsite strategy, possibly coupled with internal, open systems solution. Back up via VAN and tape.</td>
</tr>
<tr>
<td><strong>IMPORTANT</strong></td>
<td>Suspension of some business operations at the hospital but no direct impact on clinical care, patient safety, critical govt. services</td>
<td>24 - 72 hours</td>
<td>Traditional hotsite strategy, possibly coupled with internal, open systems solution. Back up via VAN and tape.</td>
</tr>
<tr>
<td><strong>DEFERRABLE</strong></td>
<td>Minor inconveniences to business operations</td>
<td>&gt; 72 hours. May not be recovered until migration to the warm site, or the original site is repaired.</td>
<td>Standard backups and restore procedures typical of component failures. Back up via tape.</td>
</tr>
</tbody>
</table>
Disaster Recovery Plan
Start your plan by identifying key assets. This will include an inventory of all IT equipment such as computers, associated hardware, and telecom equipment. Be sure to have good documentation of your network infrastructure with up-to-date network diagrams. You want to list components such as:

- Fulfillment system, product order inventory and related items
- Email system
- Files, documents, images on your network

Also, list non IT-related office equipment. Be sure to include the value of everything on the list.

Determine how the loss of each item will affect the business and the best protection needed for each.

Security Policy
Be sure to address data security issues and vulnerabilities. Understand your current network and what risks you may be exposed to. It's advisable for a third party to conduct a security assessment and help you create a plan that is understood by everyone in the company.
Steps to an Effective Business Continuity Plan

Disaster Recovery Plan (cont.)

Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are critical metrics that need to be determined when creating a disaster recovery and business continuity plan.

Recovery Time Objective
This is the estimated amount of time it will take for systems, applications and/or IT functions to recover from a disaster. Different functions will have varying RTOs. Figuring out how quickly recovery needs to happen will determine the type of preparations required such as how data is backed up and stored, a relocation site, and staffing and personnel information.

Recovery Point Objective
This is the number of hours or days in which systems and data would be restored after a disaster based on current operations. This information can be used to develop backup strategies, and to determine the amount of data that may need to be recreated after the systems or functions have been recovered.

The more specific one can be with the time required for both RTO and RPO, the more likely the business will successfully recover from a disaster.
Implement Solutions
The plan needs to include information on how to implement it. Employees and any related personnel should be very familiar with their roles and responsibilities including:

Communication
Who is responsible for communicating information? Who is the information to be communicated to? Employees? Customers? How will it be sent? Have alternative communication methods been included in the plan and what are the procedures that will be activated?

Should the company sign up with a third-party conferencing and emergency communications service? Which personnel are allowed to speak to the media?

Location of Critical Components
Maintain detailed records of hardware, software, network equipment, emergency supplies.

List of Passwords/Access codes
Steps to an Effective Business Continuity Plan

4 Implement Solutions (cont.)

Emergency Contact Information
Include contact information and regularly update it for the following:

- Police Department
- Fire Department
- Ambulance
- Gas and Electric Company
- Water Company
- Insurance Company
- Employees
- Vendors

Alternative Worksite-Hot, Warm or Cold?
Should a disaster make your company’s office space unavailable, having plans in place for an alternative worksite will be a key factor in recovering from a disaster. There are various types of sites if the office is no longer available:

**HOT SITE:** A facility that’s powered up with computers, telecommunications and the environmental infrastructure required to run a business.

**WARM SITE:** A facility with some hardware and communications interfaces, electrical and environmental conditioning, which is only capable of providing backup after additional provisioning, software or customization is performed.

**COLD SITE:** A site that contains physical space and building infrastructure. Everything must be brought in to do business. Other terms used to refer to this type of site: Backup site, Recovery site, Alternate site.
Steps to an Effective Business Continuity Plan

Test Plan
Periodically test and audit your disaster recovery plan. The plan won’t do any good if it’s old and collecting dust on the shelf or in someone’s files. Frequent testing for multiple contingencies ensures that it will actually work if disaster strikes.

After testing ask the following:
• Were the test objectives met?
• What problems were encountered?
• During the test, were there deviations from the plan?

Based on the above information:
• Revise and update plan
• Modify and/or replace solutions
• Keep strategies and solutions current
• Assign the right people to the right tasks
• Be sure the plan and procedures are easily understood so a non-IT person can implement it.
## Test Plan (cont.)

### Disaster Recovery Planning Checklist

<table>
<thead>
<tr>
<th>Action</th>
<th>Assigned To</th>
<th>Completed</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data backup and storage information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network infrastructure documentation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency contacts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Back up communications service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency supplies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>List of passwords/access codes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternative worksite</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plan tested</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IS YOUR DISASTER RECOVERY PLAN READY?

Visit us online or give us a call to request your Free Disaster Recovery Plan Assessment.

We will come to your site and review your Disaster Recovery Plan to test its readiness. Even if you've tested your plan, an independent review can point out assumptions that may spell trouble for you in the future.

(800) 339-0690
www.clarecomputer.com