

Developing your Plan

If you're putting together a continuity plan, you can get a head start by using this checklist of critical elements. Here are the key elements AGJ recommends that your enterprise can cover in its business continuity plan.



Recognize that data is an asset

Corporate data should be viewed as a key strategic asset. Inquiries from potential customers, financial transactions with existing customers, customer service communications, and new product and service marketing opportunities are all best served by a pro-active approach to data quality throughout the enterprise. Simply capturing and storing data is insufficient. Like other corporate assets, data and information quality needs to be effectively managed.



Contact information for your phone service, vendor telephony equipment and IT vendors

Your Information Technology Team includes both your inside staff and outside consultants. Do you have all the necessary information available to contact these individual in the event of an emergency. Find a contact within your local support companies who is smart and outgoing and build a relationship with them. Such actions will go a long way toward getting a quick response out of the service rep when you need them.



Contact information for IT staff and vendors

Which vendor do you have a good record with, someone who can get you the equipment in a heartbeat? Because of lead times, this is probably not someone like Dell or Hewlett-Packard but your local vendor who can supply the necessary equipment right away. Be sure to have another contact in a different area since natural disasters will undoubtedly affect local vendors in your area.



Data backup is the key

Recognized backup solutions include tape drives, external storage (e.g. USB drives), and offsite backup facilities. 70% of all businesses with backups don't test their backup solutions on a regular basis. Remember to restore your data to an alternate test PC or test folder on a routine schedule to verify that backups are working as designed.



Other Backup Considerations

Make sure your data backups and software backups are protected at an offsite location. In the event of a total hardware failure, make sure you have the software and hardware necessary to perform a full recovery. Data without the applications in most cases is useless.



Vendor Contact Information

Make sure you have contact information for ISPs, electricians, carpenters, plumbers, a PC repair service (if it is outsourced), a copier vendor, an alarm or security company, and anyone else who services or sells equipment to you. Also, you probably want to have contact information for your suppliers and

distributors. That way, you can stop, delay, or reroute the shipment of materials and notify distributors of any delays or changes in plans. Keeping them in the loop as you go through a crisis situation will reduce the amount of business lost by having them go elsewhere.



Step-by-step plans and timeframe if an office needs to be set up in an alternate location

If you have to move your offices, you will need to know what has to be in place at the new location, as well as what has to be salvaged from the old location. Identify places you can move to ahead of time, considering such things as security at your new location and, depending on the emergency, additional security at the old location to prevent theft and looting.

Other items to consider here are the routing of phone lines, dedicated Internet access lines, notification of postal services, distributors, suppliers, and letting all employees know where to report to work.



Sample forms for taking messages and processing any other information your company uses, such as order and dispatch service forms (You want to keep running, don't you?)

Instead of handing out blank pieces of paper and pens to take messages and place orders, hand out formatted pieces of paper to take this information down. By having prompts and spaces for all pertinent information, you reduce the amount of mistakes by people who may not be thinking too clearly during a crisis. Also, if you are hiring temporary employees to help in a crisis, these types of documents will allow them to help you with minimal training needed.



A hierarchy of critical services and infrastructure to determine what should be brought online first

When the IS department thinks that e-mail is mission-critical and the marketing and sales department feels that the fax machine is most important, an agreed-upon schedule of which services should come online first will help determine priorities. A simple planning meeting to assess your infrastructure and determine which systems are more important than others will allow you to create a list of what areas to work on first when you have to start from ground zero.