c3group | Preparing your best Disaster Recovery Plan

It's hard to have a perfect, fool proof plan. The points below are simply guidelines to consider when prepping for your complete plan. We recommend thinking about each point, and taking your thoughts to your IT Provider, so you can work with them to ensure your tech environment correlates with your desired outcomes & process, should your experience a disaster.

☐ **Risk Analysis:**
• Conduct a risk analysis of your computer systems. List all the potential risks that threaten your system up time, and evaluate how imminent they are in your business operations. Remember that anything that can cause a system outage is a threat; from relatively common cyber or human threats like virus attacks and accidental data deletions, to more rare natural threats like floods and fires.

☐ **Identify who does what when a disaster strikes:**
• This is generally a list of key stakeholders, executives and managers, along with disaster response responsibilities; so think about who will monitor your disaster status and talk with third party remediators, who has authority to make decisions, what needs to be completed in each department to restore operations? etc.
• Your plan needs spell out who will be responsible for what, as a clear plan and response times are critical.

☐ **Plan for people & determine equipment needs:**
• What will your employees do if your business experiences downtime?
• If you're trying to operate critical business areas during a disaster, what team members do you require to continue working, and what & how many devices would you realistically need? Where do you get them from?

☐ **Ensure your critical data is safe:**
• It's important to backup data in multiple locations, such as the cloud, on servers, and on premises. The location will affect certain performance metrics, including failover times and how quickly files can be recovered.
• It's important to know what assets you need to be available quickly, and what can wait. This will be different from business to business, consider cloud continuity for the mission-critical systems.

☐ **Have a backup office:**
• Considering where or how your critical staff would work if your office is unavailable will not only save you costs in paying full-time staff during downtime, it will also allow for crucial work to flow as normal – meaning there'll also be no affect to your client satisfaction and your reputation.
• For some businesses, having BYOD (bring your own devices), and utilising cloud & business continuity will take care of this completely.

☐ **Communication is key:**
• Ensure your people are aware of your disaster recovery plan.
• Know which stakeholders you need to contact to begin the execution of the disaster recover plan.
• Make sure devices that need to be used are easily attainable.
• Ensure your teams know how to communicate in the instance of downtime; if emails and phones are offline, what will they do?
• Know what you'll say to the outside world. Just as important as internal communication, is external communication. If your business has a large impact on the running of other businesses, or your clients will be affected, how will you let them know you're working on minimal resources until you're back up and running.

☐ **Constantly re-evaluate & test:**
• Disaster preparedness is a work in progress. You need to constantly re-evaluate your plan to ensure that you're planning for all possible scenarios, and incorporating any changes within your company / team environment.
• While tests are disruptive, they're necessary. The test itself is usually simple: turn off systems, then follow your plan. Things can easily go wrong, especially for the initial test, so choose a test time wisely, and have a Plan B should your process not go quite according to plan.