Austin Technology
3/52 Frobisher St
Osborne Park, WA, 6017

PH: 1300 787 429
support@austinechnology.com.au
www.austintechnology.com.au

How to Build a Disaster Recovery Plan

Disaster can strike at any moment, and its effects can be devastating. A study sponsored by Symantec found that each individual breached record costs a company an average of $188. The accumulated costs of data loss can easily total thousands, or even millions, of dollars.[1] With such consequences, it is critical to have a solid disaster recovery plan in place in case the worst happens. However, 40% of small businesses do not have such a contingency plan, according to the National Cyber Security Alliance.[2] A good disaster recovery plan has three parts: Planning, Storage, and Recovery.

Planning

A solid disaster recovery plan requires everyone involved to know their roles and be ready to execute them at a moment's notice. At the very least, your business should designate someone to ensure that all preparations are laid out and that all critical data is backed up regularly. Ideally, this person will be someone other than you, since you as the business owner will want to go back and double check their work for redundancy.

Redundancy is a key aspect of planning for disaster recovery - always make sure that there are redundant channels and oversight. Channels of communication need to be set up so that everyone knows who to call as a primary contact and who to get in touch with in case that person cannot be reached. Keep cell phone numbers on hand in case text messages are the only way you can reach each other, which can happen when entire cities lose power due to a natural disaster. Maintaining a strong chain of communication can mean the difference between a temporary outage and a major business catastrophe.

Storage

Storing your data securely for a post-disaster recovery is as important as planning. The first step to storing and protecting your data is choosing a backup and storage method and provider. There are many options available for both backup and storage, and choosing the right one is based largely on the needs of your business.

Larger companies with more intricate data needs and in-house IT staff require different solutions than smaller organizations. Regardless of your organization's size, it is important

[1] https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf
[2] http://smallbusiness.house.gov/uploadedfiles/kaiser_testimony.pdf

to make sure your recovery data is kept in multiple physical locations separated by some distance. Most cloud and managed backup providers already guarantee this level of duplication and redundancy by distributing your stored data across multiple different data warehouses in multiple locations. However, if you go with an in-house or custom solution, it is important to make sure that backups are not all located in the same data storage facility, and certainly not in the same building as your offices.

Depending on the sensitive nature of the data you are backing up, you may have additional requirements such as encryption or other security measures. In such cases, your data would not only need to be encrypted when it is stored, it will also need to be encrypted as it is transmitted to the backup location.

Recovery

The process of recovery begins with a good policy of detection and monitoring. Make sure that your disaster recovery plan accounts for careful tracking of your data in case of fires when you are out of the office, malicious intrusion (either physical or cyber), power outages and other issues. The faster you learn that your data is in danger, the quicker you can react and the easier the recovery process can be.

40% of small businesses do not have a contingency plan in case of data loss.

Remember, everyone on your staff should know whom to contact in the event of a major disaster. Make sure to inform your staff that their safety is the top priority - if you have been backing up your data properly and storing it offsite, losing your equipment in a disaster is only a temporary setback. Make sure you know where your data is and how to retrieve it. Practice full recovery drills periodically with your team or service provider so that everyone on your staff knows what to do - you do not want to have to add learning an unfamiliar system to all the other post-disaster stress.

Make sure you have a plan about what needs to be recovered first, where all your priority information is, and how to get to it. For many businesses, this will be websites, client portals, and any information that needs to be accessed by your customers. It should also include your most sensitive business information.

Having a disaster recovery plan can make the time between disaster and recovery much shorter than it would be without one, and the work required to implement one is minor compared to the risk of losing your business. Don't be one of the over 50% of businesses that do not make regular backups - plan for the worst, and you will be able to weather any storm.