

'10 tips for disaster recovery planning'



1: Devise a disaster recovery plan *(What do you need to put in place?)*

It is important to start with the basics and add to the plan over time. To begin, define what is important to keep the business running - i.e., email and application access, database back-up, computer equipment and the "recovery time objective" or how quickly the company needs to be up and running post-disaster.

2: Monitor Implementation *(You must keep the plan up to date)*

Once a disaster recovery plan has been established, it is critical to monitor the plan to ensure its components are implemented effectively. A disaster recovery plan should be viewed as a living, breathing document that can and should be updated frequently, as needed.

3: Test the plan *(It's no use having one unless you know it works)*

The ability of the disaster recovery plan to be effective in emergency situations can only be assessed if rigorous testing is carried out one or more times per year in realistic conditions by simulating circumstances that would be applicable in an actual emergency.

4: Back-up off site *(Are your back-ups kept off-site?)*

The primary concerns for data back-up are security during and accessibility following a crisis. There is no benefit to creating a back-up file of valuable data if this information is not transferred via a secure method and stored in an offsite data storage centre with foolproof protection. Every company should back-up its data at least once daily.

5: Perform data restoration tests *(Do you know that your back-ups work?)*

However you back-up, the software and the hardware on which it resides needs to be checked daily to verify that back-up is completed successfully and that there are no pending problems with the hardware. Companies need to perform monthly test restoration to validate that a restoration can be accomplished during a disaster.

6: Laptops and Desktops *(Is there critical data kept on them?)*

Although many companies have policies requiring employees to store all data on the company's network, it is not prudent to assume that the policy is being followed. Backing up laptops and desktops protects critical data in the event of a lost, stolen or damaged workstation.

7: Be redundant *(Do you have a redundant server in place?)*

Establishing redundant servers for all critical data and providing an alternate way to access that data are essential components of an organization's disaster recovery planning. Having these redundant services in place at a secure, offsite location can bring disaster recovery time down to minutes rather than days.

8: Invest in theft recovery *(What would happen if your laptops went missing?)*

Unlike desktops, laptops are more easily misplaced or stolen. Theft recovery solutions can locate, recover and return lost or stolen computers, while data delete options can enable companies to delete data remotely from lost or stolen computers thereby preventing the release of sensitive information.

9: Regular updates for your Anti-virus *(Are you sure all your systems are up to date?)*

Companies often do not focus on email security until an incipient virus, spyware or malware wreaks havoc on employees' desktops. Organizations need to protect its data and systems by installing regular virus pattern updates as part of disaster recovery planning, which may even help prevent a crisis from happening.

10: Use the professionals *(Make sure you get professional advice?)*

Managed services providers have the technical personnel to design, implement and manage complex disaster recovery projects.

If you would like to talk to Active about how you can implement a disaster recovery plan for your business then please contact us on 01403 740400.

