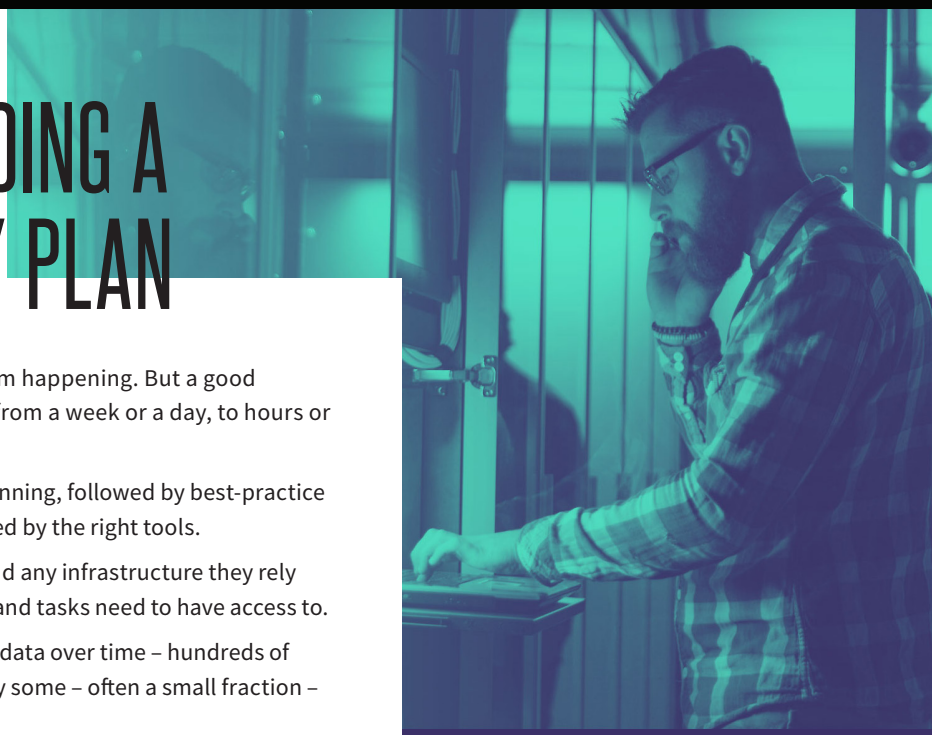
arcserve®

eBook

HOW TO BUILD A DISASTER RECOVERY PLAN

BEST PRACTICES



SUCCESSFULLY BUILDING A DISASTER RECOVERY PLAN

No amount of money or planning can stop disasters from happening. But a good disaster recovery (DR) plan can reduce your downtime from a week or a day, to hours or even minutes.

Like any important project, successful DR starts with planning, followed by best-practice templates and procedures, which in turn are implemented by the right tools.

In addition to identifying mission-critical applications and any infrastructure they rely on, you should also identify the data these applications and tasks need to have access to.

Your company has accumulated a substantial amount of data over time – hundreds of gigabytes, perhaps terabytes or even petabytes. But only some – often a small fraction – of this data has to be made available again quickly.

STEP 1: Business Impact Analysis

A Business Impact Analysis (BIA) defines what capabilities your company can't operate without. This is the first step in creating a working disaster recovery plan.

Doing a BIA must involve top-level, non-IT management, to identify and agree on the list of applications that are considered essential, and IT management to map these tasks against the applications along with the associated infrastructure and other services needed to run and use these applications.

All top stakeholders must be involved in the analysis. You don't want to find out after a site goes down that there was an additional application an executive considers essential.

STEP 2: Risk Assessment

The second step to a complete DR plan includes mapping the two types of IT infrastructure:

1. IT infrastructure you control, whether located in your offices or in co-location facilities.
2. IT infrastructure you don't control – like web and cloud services or web sites running in a hosted environment.

Once the IT infrastructure has been mapped, look for single points of failure, like a server with only one network card.

These are your first places to consider "fortifying" with redundancy.

WHAT CAUSES IT DISASTERS?

The cause of an IT disaster may be small and specific. A power supply, CPU, network interface card, RAM, fan, or other component on an individual server may fail. A brief power fluctuation may scramble data or disrupt a program's activity.

An entire data center going down is rare, but can happen. Weather may take down external power or network service. The resulting fire, flood, or building damage may bring down your entire computer room or data center.

STEP 3: Risk Management

To lower the risk of an IT disaster occurring, fortify yourself against the most common issues and you will have protected yourself against 90%-95% of the small incidents that may impact you.

Redundancy is one popular approach to avoiding, or minimizing, many IT disaster events. For example, servers, storage and network gear can be configured with two power supplies, connected in turn to separate power sources. Servers, firewalls, UPSs and other gear, even entire sites, can be duplicated. Network and electrical service can be supplied by two separate utilities, on separate cables. Data can be stored across multiple hard drives.

STEP 4: DR Testing

There are only two ways to determine whether a DR plan works.

One is when there's a disaster. This, of course, is the wrong time to discover that you chose wrong, or that one of your tools or services has failed, or that you didn't include a critical application.

The other way is to periodically conduct tests. It is better to uncover a shortcoming in your infrastructure by testing failure scenarios under controlled circumstances.

External audits can help identify whether there are any parts of your DR plan that still need work. One reason is that not all organizations will simulate a full disaster scenario, or carry through to confirm that a full recovery can be done. An external audit can hold you to a higher standard than your company may have set, and conduct full, rigorous tests, forcing you to follow the best IT practices.

Offsite Backup Approaches

In most IT disaster events, disaster recovery involves restoring data, because the primary copy has been damaged, destroyed, or rendered inaccessible.

To ensure that a copy of your data is available if and when an IT disaster occurs, an offsite backup is critical. It should be geographically far enough away to ensure that a major event like fire, flood, power outage, explosion or earthquake doesn't damage or isolate the backup.

Tape ruled the offsite backup world for decades. But there are challenges with tape-based backups:

- Offsite tapes take time to request, find, and retrieve.
- If a tape is faulty, you don't find out until you need it.
- To read older-generation tapes, you need to have a working tape drive that supports them. Since your site may be inaccessible, you need one at your alternate location as well. This adds to infrastructure costs.
- You may have to go through the entire tape just to retrieve a few files.
- Many tape-oriented backups use proprietary formats, and require vendor software to be read – another recurring cost.

In today's online, 24x7x365 world, a backup that's not quickly and easily available may be good for preserving important company data – but it isn't useful for disaster recovery. Today's RTOs are measured in hours or even minutes.

RECOVERY POINT OBJECTIVE (RPO) AND RECOVERY TIME OBJECTIVE (RTO)

The data that you want to regain availability to in a timely fashion is called the Recovery Point Objective (RPO).

How soon you want this data available again is called the Recovery Time Objective (RTO).

How much IT downtime for mission-critical applications and data is acceptable depends on many factors (notably cost), and will vary from one company to the next -- but in general, acceptable downtime today is minutes-to-hours, compared to days to a week or more from years ago.

HOSTING APPLICATIONS VS. OUTSOURCING

Another critical component of managing the risk of IT disasters is assessing whether it's time to outsource any of your IT applications and services, and move them to the cloud.

ABOUT ARCSERVE

Arcserve provides exceptional solutions to protect the priceless digital assets of organizations in need of full scale, comprehensive data protection. Established in 1983, Arcserve is the world's most experienced provider of business continuity solutions that safeguard multi-generational IT infrastructures with applications and systems in any location, on premises and in the cloud. Organizations in over 150 countries around the world rely on Arcserve's highly efficient, integrated technologies and expertise to eliminate the risk of data loss and extended downtime while the reducing the cost and complexity of backing up and restoring data by up to 50 percent. Arcserve is headquartered in Minneapolis, Minnesota with locations around the world.

Explore more **arcserve.com**

MAKE DR DOCUMENTATION AVAILABLE

There's a lot of information associated with a disaster recovery plan. One example is contact information for vendors, your employees, utility companies, and other organizations you may need to talk with. Another is IT equipment inventories, including serial numbers and warranty information, circuit IDs, building maps, etc.

Make sure that you have copies of this information that you can access even if all your regular IT – and possibly the wired and wireless phone networks – is offline. Consider storing a copy online, and also keeping a secured copy on your smartphone, tablet or notebook, and on a flash drive.