Right Networks®

eBook

Disaster recovery plan to back up data

Have a data backup plan as a disaster recovery strategy

Disasters are inevitable. They can happen at any time—even right now.

Sure, you might see a natural disaster coming and be able to react, but what about coffee spilled into a laptop? A burst pipe flooding your office or home office? Or something most people don't even think of as a disaster: data theft. But if data is unavailable—or worse, lost—it's a disaster.

Chances are that at some point it'll happen to your firm. The random true stories are nightmarish and all too common. A reporter for a magazine once had to replace a computer after juice from the can of peaches he was eating splashed into his keyboard. Then, there was the publishing company west of Boston, where the office flooded when a pipe burst in an office upstairs. Employees scrambled to dry off computers and get servers off the floor and onto desks as water flowed down and pooled on the carpet.

Sometimes nature itself is just too strong. Wildfires now rage regularly in the American West. Earthquakes are a constant threat in some parts of the U.S. Or consider this story from recent deadly flooding in Kentucky: An official from a church denomination received a call from a pastor in the eastern part of the state. The pastor had stored all her sermons and writings—a lifetime of work—on an external hard drive that sustained flood damage. Nothing was backed up anywhere else. Most, perhaps all, of those files are gone forever.

Businesses without a data backup strategy often don't survive data loss

A data disaster can devastate a business or a firm like yours. A **2019 LogicMonitor survey** showed that 96% of businesses had experienced an outage in the three preceding years. The survey also revealed that half of those outages were avoidable.

Outages are expensive, too. A **2022 survey from Veeam** pegged the cost of an outage at $1,467 per minute, or $88,000 per hour.

Disasters often cause outages, which can devastate firms and other businesses. Luckily, in many cases, companies that suffer outages don't actually lose any data. They just don't have access to it when they need it (which is bad enough on its own).

However, losing the data itself is another issue altogether—and something a firm simply cannot afford to have happen.

Statistics show exactly **the kind of damage data loss does to businesses**:

- 93% of companies that experienced a datacenter outage for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster. (National Archives & Records Administration in Washington)
- 94% of companies that suffered a catastrophic data loss did not survive; 43% never reopened and 51% closed within two years. (University of Texas)
- 30% of all businesses that suffer a major fire go out of business within a year, and 70% fail within five years. (Home Office Computing Magazine)

Your accounting firm, like all businesses, needs a comprehensive plan in place for data backup and recovery. It's important, of course, to protect data to the greatest extent possible. But, again, disasters are inevitable. The key when one happens is to be able to access and recover data as soon as possible after the incident—and never lose any data at all.

Data-loss catastrophes go beyond data breaches and natural disasters

When you think about events that could lead to data loss, you might think about data breaches that lead to theft of information. Indeed, breaches are one of the leading causes of both downtime and data loss. Even companies that pay exorbitant ransoms after falling victim to ransomware attacks don't always get their data back. If your firm isn't equipped to **prevent data breaches**, you need to rectify that situation right now.

But most firms do have some measures in place to at least mitigate damage from data breaches. The same goes for another common cause of data loss: viruses. Every firm has some sort of antivirus technology in place and has for years.

So, what are the **causes of data loss** firms might not see coming?

For one, employees can go rogue and save files on individual hard drives rather than storing them in folders backed up in the cloud. It's easy to slip occasionally and forget to save a critical file in a cloud-enabled area. In those cases, stress and the pace of work can lead to disaster, as the Kentucky pastor sadly discovered in what was an extreme case but one that happened nonetheless. Firms need to back up individual computers as well as information resting on servers.

Hard drives can die in all sorts of ways. Theft, a fire or flood, or even unintentional abuse from a user can end a hard drive's life. And sometimes they just fail. Like all pieces of technology, a hard drive is not guaranteed to work all the time, forever. It's possible, sometimes, to recover information from a failed hard drive, but it's costly and time-consuming. And there's no guarantee of getting everything back.

Another major cause of data loss involves something we've all likely done—accidentally deleted a file. Computer users, it turns out, do this all the time. Fishing a file out of a recycle bin isn't that hard to do, but what happens when the file isn't there, either? It's probably gone forever.

Accidental deletions even happen with files stored in the cloud. Also, even the most astute of users can sometimes accidently overwrite a file or drag it into the wrong directory, leading to data loss and a need for recovery. That's why the ability to recover an inadvertently deleted, misplaced or replaced file is so critical and something a good cloud provider should absolutely offer.

Then there are the truly unexpected causes of data loss. Power outages or surges can zap an individual computer or even an in-office server and obliterate data in an instant. And then there's that bracing cup of morning coffee. If the java ends up dripping into a laptop or, heaven forbid, seeping into an office server, data is at severe risk of disappearing. Do you take sugar in your coffee? That actually makes it worse. (Beware of canned peaches, too.)

How to come up with a data backup plan for disaster recovery

How prepared is your firm to recover data after a disaster? You might not even know. Fortunately, there is a template firms can use to develop a data-recovery plan. Roman Kepczyk, security expert and director of firm technology strategy for Right Networks, advocates for a **3-2-1 backup strategy**.

Before you get to the countdown, start by taking stock of what your firm already has in place. If you are still relying on physical media—such as a solo network-attached storage (NAS) drive, flash drives, DVDs or even actual tapes—your firm is at risk. Those backup types most often require the constant physical intervention of creating and verifying the backups and taking them off-site to a secure location.

Within many accounting firms, there is seldom consistent follow-through on manual backup procedures, particularly when the person primarily responsible for doing so goes on vacation or there's a staffing change. Modern backup solutions are automatic, verify that the process is complete and notify firm members if there is a problem or anomaly that requires attention.

Now the countdown comes into play. The best way to ensure that your data is backed up and available is by partnering with a cloud provider for backup and not trying to do it yourself. But even when a cloud provider is involved, the basic 3-2-1 rules still apply.

3. You should have a minimum of three different copies of data (your original production data and two backup copies) in addition to any archival copies you plan to keep.
2. Your copies of data should be stored on at least two different types of media (i.e., NAS, cloud).
1. You should keep at least one copy off-site (such as a secure location or in the cloud). Best practices also recommend that at least one backup is air-gapped (where backup is physically or virtually disconnected from the network) and immutable (where backup is in a state in which it can't be changed in any way). These features, available with modern backup solutions, are designed to counteract a ransomware attack.

Rely on a secure cloud infrastructure for your data backup strategy

Frankly, it's going to be hard—nearly impossible, in fact—for you to pull this off on your own. Moving at least some backup capabilities to the cloud is the best option by far. Physically moving backup media off-site is fraught with problems, including user follow-through, accessibility and security. That's why firms should evaluate cloud solutions that automatically back up data off-site via an encrypted fashion.

While backing up all files via the internet can take a significant amount of time, cloud providers allow for more rapid intermediate backups to be incorporated during the week, with full weekly backups being conducted on weekends to minimize impact during working hours. Intermediate backups during the week include differentials, which are backups of all files that have changed since the last full backup.

Cloud providers integrate different intermediate backup solutions to restore more efficiently and rapidly both individual and full system files, leading to faster data recovery for your firm. The latest cloud solutions can also restore data to a virtual environment where your firm can run the applications remotely, similar to how cloud applications and hosting providers themselves function.

The time and resources necessary for implantation and maintenance make managing backup and recovery in-house difficult (to the point of being nearly impossible, quite honestly). Cloud providers, on the other hand, offer a safer, more cost-effective and less difficult way of making sure your firm's data is available under just about any circumstances, no matter how dire.

Why cloud backup is the best way to protect critical data

There are other reasons why cloud backup makes sense. The benefits go far beyond ease of maintenance. Consider other advantages of backing up data in the cloud:

It gives you an open global work environment: As remote work becomes more commonplace, companies have started to look beyond their immediate geographical areas to seek talent. This is occurring alongside the growing international use of cloud services overall. With cloud backup, your firm can safely access data from any point of origin no matter what happens in an individual office or someone's home.

Your information becomes portable: Workers who travel for business can access their company database virtually, effectively placing needed information at their fingertips.

You can grow your brand: As clients have become savvier, they have come to rely on firms that have modernized and automated their workplaces. In other words, firms that use modern methods like automatic backups can grow their brands and increase name recognition.

It increases client trust: Your clients will appreciate you for improving your processes to keep their information safe. You'll also be able to secure new clients who are aware of what you're doing that other firms might not be doing.

It significantly reduces risk: The buzzword for modern firms is "Security, security, security!" Backup is a critical element of security, and cloud backup massively reduces the chances of data loss.

Your data is protected from all sorts of disasters: A cloud provider's enterprise-class datacenter facilities give your information storage space that's safe from fires, floods, equipment theft and other types of data disasters.

Choose the right cloud hosting solutions for data backup and recovery

The important thing, then, is to find a cloud provider you can trust. After all, cloud backup is only as safe as the provider that's protecting your data. Downtime costs money, even if it's your cloud provider that's experiencing downtime or not getting you access to your data as quickly as possible after a data disaster.

Right Networks has two decades of experience backing up and recovering data. Our **cloud hosting** and **Secure Workstation** products have everything your firm needs to withstand a disaster, including data storage in Tier 3 and 4 datacenters, real-time data replication, and automatic backups. With Right Networks, your firm will be ready for whatever comes next.

Any business that deals with financial data needs to store information in Tier 3 or 4 datacenters. Tier 1 and 2 datacenters offer less uptime and less protection against power outages and other potential data disasters. A Tier 2 datacenter, for instance, is likely to have 13 times more downtime in a given year than a Tier 3 datacenter.

Or consider our comprehensive security offering, based around the concept of **Smart Security Management**.

- **Accounting and tax application cloud hosting:** Secure and reliable cloud hosting that safeguards your data with end-to-end redundancy across all systems, real-time data replication and enterprise-class multi-layer security systems—24/7/365.
- **Secure Workstation:** A comprehensive, secure endpoint solution to safeguard your business-critical data. You can have peace of mind with added security for all your employees with one enterprise-level solution.
- **Security Awareness Training:** An employee education program that provides best practices for staying safe online using an expert-developed gamified training program.

Right Networks offers technology, expertise and training from a single organization that has been at the forefront of securing accounting firms for more than two decades. Firm leaders can turn the essential task of managing security over to a trusted partner and get back to doing what they do best: serving clients and running their firms.

QuickBooks® Online users have a trusted backup option in **Rewind**, a Right Networks partner. Rewind automatically backs up QBO files so you can restore any QuickBooks file you need whenever you need it without downtime—and gain the data security compliances that QBO alone can't offer.

A data disaster could happen at any time. It could come from the sky, from the office upstairs or from a simple cup of coffee. And it could spell doom for your firm. But you can be ready for anything with cloud backup from Right Networks.