Wait, Where Did My Files Go? (The Importance of Backup Procedures and Disaster Recovery)

by Makaela Rae Clapp, CPA, Staff Associate II

Posted on July 13, 2022

Have you ever found yourself in a situation where you realize that you have lost important digital files – maybe a picture was accidentally deleted or your phone broke? It is always disheartening to lose access to your important files. But have you ever considered the impact if this were to happen in the workplace? As information has increasingly become digitized, all organizations have been navigating how to manage the sheer volume of files and data they accumulate. Storing information digitally provides many benefits – fewer file cabinets taking up space, you don't have to worry about a fire or flood destroying paper documents, files leave an audit trail, etc. However, in order to reap these benefits, you must ensure that your organization has proper backup procedures to alleviate the risk of data loss and keep sensitive data secure. In addition, sufficient backup procedures can help your organization to continue operating in the event of a disaster. The following is a non-exclusive list of events that could happen at any time:

- Hard drives could fail.
- Computers stop working.
- Devices get stolen.
- Human error could result in the loss of data accidentally.
- Networks could be infiltrated by a virus, or other cyberattacks could occur where data is stolen.

- Disasters could happen that could potentially shut down technology from working or prevent employees from accessing physical hard drives.

We really hope that these events will not happen, but it is crucial to be prepared in the event that they do. So, how can we best prepare? According to Cloudian, there are many methods to back up your organization's data.

1. **Removable media:** This includes flash drives, CDs/DVDs, and tape backups. These are most beneficial for smaller items or organizations.
2. **Redundancy:** This method requires creating a replica of your existing hard drive or entire system. This can be beneficial but requires a lot of effort to continuously duplicate information.
3. **External hard drives:** External hard drives can hold large amounts of data, but you may need multiple depending on your organization's size.
4. **Cloud backup:** Utilizing the cloud is a strong choice as your data is stored offsite in a remote location, and data centers can hold massive amounts of data. This is also referred to as Backup as a Service (BaaS). The cost is definitely a factor as you would need to pay a vendor to store your data, but the security you receive is valuable. Your data would be safe if a disaster occurred at your onsite location, and you do not have to worry about the hassle of storing the data. It is also easy to access your data online.

As a best practice, most organizations should be backing up their data weekly at a minimum or daily if possible. According to ioSafe, there are also a few types of backups, including full backups, incremental backups, and differential backups. A full backup makes a copy of everything, but it takes the most time and network bandwidth. The best strategy for organizations that use large amounts of data is to do an encrypted full backup initially and then perform incremental or differential backups regularly. Incremental backups only make copies of new data since the last full backup. Alternatively, instead of having multiple incremental backups saved, you could perform a differential backup which only saves the initial full backup and the latest incremental backup performed. This last method will save the most space and provide for a faster recovery of data than using all incremental backups.

Another best practice is to utilize multiple backup methods in case one method fails. A recommended strategy from Cloudian is called the 3-2-1 Backup Strategy, or Hybrid Data Backup. This method is comprised of the following elements:

- **Three** copies of data – Original data and two duplicates.
- **Two** different storage types – This ensures that if one method fails, you can still recover data via the alternate method. Usually, removable media or external hard drives are used in conjunction with cloud storage.
- **One** remote copy – It is crucial to back up data to a remote site in the event of a disaster so you can still recover your data.

You may think that you already have sufficient backup procedures, but do you know what you would actually do if something went wrong? This is where having a disaster recovery plan comes into play. A disaster recovery plan is essentially a documented procedure manual that details what your organization would do in the event of a disaster to restore system applications and enable operations to continue. Auditors check to see if you have one to ensure that your organization is prepared. Some examples of disasters could include, but are not limited to, natural disasters like floods or tornados, a city-wide power outage, or even cyberattacks. This is why having a remote backup copy is so important!

A comprehensive disaster recovery plan should generally include the following elements:

- Business impact analysis, including a risk assessment of critical business functions, risk mitigation, and disaster scenarios.
- Business recovery strategies, including recovery tasks and procedures.
- Computer equipment and software inventories.
- List of supplies, equipment, and vital records required for resumption and recovery efforts.
- Crisis management plan.
- Escalation procedures used to specify exactly how to respond to emergencies and how to tell when a “problem” has become a potential “disaster.”
- Disaster recovery plans should state the steps to follow for escalating unresolved problems to disaster status.
- Contact lists and notification procedures of recovery team members, management personnel, vendors, and others as may be appropriate.
- Plan maintenance and training requirements to ensure that the plan is kept up-to-date and all parties understand their roles and responsibilities during the plan’s execution.

Disaster recovery plans should be reviewed regularly for changes in personnel or procedures. In addition, management should test the plan at least annually to identify any deficiencies in the plan. Remember, an ounce of prevention is worth a pound of cure when it comes to critical IT systems.

If I have not convinced you about how important disaster recovery plans or backing up your data is, here are some scary statistics from the WebTribunal regarding data loss:

- 60% of businesses going through a data loss incident will shut down within six months after that.
- 93% of organizations that suffer a major data disaster and don’t have a recovery plan will go out of business within one year.
- 31% of PC users have lost all their data due to uncontrollable events.
- During the first half of 1999, American businesses lost more than $7.6 billion because of computer viruses. The risks are most likely much greater today as viruses and hackers have become much more advanced.

There is much more to be said about the importance of backing up your data sufficiently, but hopefully this overview will spark the conversation and help give you an idea of what to look for as you expand your data recovery procedures.

Related articles:

- How Strong is Your Password?
- Ransomware and the Increase of Cybersecurity Threats