What is the Best Way to Backup?

"That will never happen to me." We get through our lives telling ourselves the worst won't happen to us. It's the same with business: "We won't need this data backup." Yet, whatever your industry, secure, reliable backup ensures business as usual. So, what's the best way to backup? Here's help.

Why You Need to Backup

1. Business disruptions of any kind can be costly. The disaster might take one of several shapes:
2. Natural (e.g. wildfires, floods, earthquakes, or hurricanes)
3. On-site (e.g. hardware/software failure, power outage, inability to access building)
4. Employee driven (e.g. damaging mistakes or intentional sabotage by a disgruntled employee)
5. Cyber-attack (e.g. data breach, ransomware, or distributed denial of service attack).

Regardless, the best backup solution can help reduce downtime and damage.

Plan B: Approaches to Backup

There are several off-the-shelf backup options your business can use. Let's consider the pros and cons of the most popular ones.

USB Thumb Drives — Also known as "flash drives," "pen drives," or "memory sticks," these thumb-sized devices are compact and portable. But, they have size limitations compared to hard drives. Also, the mobility makes them easy to lose (which can actually set the disaster scenario in motion).

Additionally, a USB thumb drive is robust when not plugged in, but more vulnerable when attached. If someone inadvertently snaps the drive or employs too much force, they can put the data on that backup at risk.

The cheap ones also tend to be slow, which can make backing up sluggish.

USB Hard Drives — Portable hard drives increase the data storage available, often at a decent price. They are designed to be compact and mobile. You can prioritize durability, processing speed, storage volumes and more.

Hard drives are less likely to get damaged than a thumb drive. If knocked or jostled, the cables are flexible. Still, a hard drive can be prone to physical failure. Selecting an external solid slate drive (SSD) can help since it has no moving parts. Information is stored instead in microchips.

Cloud Storage — Backing up to the cloud stores data on an external, secure server. If thieves take your computers and USB backup, you can still access your data on the cloud. Cloud storage providers build in redundancy to ensure your backup remains safe.

Most cloud storage services back up to secure centers with thousands of servers storing data. Oh, and they'll have their own server backups too, just in case they're the ones hit by a disaster. The providers also encrypt data during transit to further ensure compliance and security.

Migrating to a third-party cloud storage service also cuts the clutter at your premises. You can count on expert help to ensure security and compliance. Plus, you can cut operational costs by offloading in-house storage or external hard drive expenses.

OK, What's the Best Answer?

Don’t think disaster won’t strike your business. Research has found data loss and downtime are most often caused by:

- Hardware failures (45% of total unplanned downtime)
- Loss of power (35%)
- Software failure (34%)
- Data corruption (24%)
- External security breaches (23%)
- Accidental user error (20%).

We recommend the 3-2-1 backup strategy. This means having 3 copies of your data. Two (2) of these would be located on different devices (e.g. on your computer and on a backup drive). The other remaining backup copy (1) would be secured offsite, in the cloud.

Want to secure your data for the worst? Give us a call at 253-881-5055 to set this up.