THE SMB BACKUP CHECKLIST

What Every Company MUST Think of to Safeguard Their Information

By Monique Phalen, Director of Technology, AIS

IMAGINE IF ALL OF YOUR BUSINESS DATA SUDDENLY WAS LOST.

Think about that just until you start to break into a cold sweat. If you aren't backing up your company data with a consistent plan, the possibility of losing at least some of your critical business data is possible—maybe even probable. How often does lost data affect businesses?

Research from Ponemon Institute revealed that 78% of companies had a data breach in the two years before the survey that lead to data loss. This lost data does real damage to your business. ESG research shows data loss leads to:

- Lost opportunities—25%
- Dissatisfied customers—23%
- Direct loss of revenue—21%

One of the certainties in life is that IT equipment—the servers where your data lives—will wear out and eventually fail. Yet many small and medium businesses don't have a plan to backup their data at all. This doesn't have to be you.

We've put together this short guide with 14 things you need to consider when it comes to backing up your business' data.

CLICK HERE TO SHARE →

AND WHAT ARE THE LEADING CAUSES OF DATA LOSS?

- 44% hardware failure
- 32% human error
- 14% software error
- 7% virus
- 3% natural disaster

Before we get to the checklist, let's make sure we're all on the same page when it comes to

DATA BACKUP

Most people think of disaster as something out of the ordinary. A disaster in a business sense is anything that keeps your business from running. Information technology is prone to breakage—whether from aging equipment or improper setup, research shows that it happens frequently.

Case in point, one of our newest clients experienced downtime while in the process of switching to our IT services. The first experience was due to a server crashing because of an out of control system process. The last one was due to existing hardware that was improperly configured. This is just an example of what we have seen but downtime "disaster" can strike when you least expect it.

Data can be lost due to malicious intent (hackers, viruses, or disgruntled staff), a disaster, or straightforward incompetence and bad luck.

CLICK HERE TO SHARE →

WHAT IS DATA BACKUP?

Data backups can take many forms. Simply put, they are copies of your files that you create in case you lose your data. This can be an in-house IT function or a managed IT service. These copies may be to hard drives, servers, cloud services, or to removable media (such as tape) for storage. The exact backup method and frequency depends on your company's storage requirements, how much data you're working with, how to treat different types of information, and the resources you have on hand. Backups can be hourly, daily, or weekly and you should store backup data in a separate location for redundancy. It doesn't do you any good to have your backup tapes sitting next to your servers in your server room if there's a fire.

WHAT IS DISASTER RECOVERY?

Your organization faces many threats that could take out your technology infrastructure. A disaster recovery plan establishes the steps you take to restore your business to an operational state. If your systems go down, or you no longer have critical data available, you face a broad range of disruptions. Disaster recovery focuses on minimizing productivity and revenue loss with a known procedure for getting your business back on its feet.

WHY DATA BACKUP ALONE ISN'T ENOUGH FOR DISASTER RECOVERY

Disaster recovery is broader than your data. A data-centric approach overlooks many important details, such as how to restore your telephony system or how long it takes to restore your data due to its geographic location. Dozens of details go into a disaster recovery plan that will actually protect your business from the unexpected. For instance, you're not going to survive a disaster intact if you copy data onto hard drives stored at a location destroyed in a fire, or if you only back up every few months.

With these differences in mind, let's explore the 14 things you need to do to protect your business...

#1 BACKUP YOUR DATA – HAVE A PLAN!

It's amazing how many companies simply don't backup their data—and we're not talking about backing up your laptop or PC. So the first step is simply this: have (and follow) a backup plan.

Symantec research shows that only half of businesses backup more than 60% of their data. For SMBs, it gets worse. Gartner reports only 35% have a backup plan—that means nearly 6 out of 10 of you reading this don't have a backup plan at all. *[Hint: GET ONE!]*

In the all too likely event of a system failure of some kind, even for the businesses that do backup data, they could lose up to 40% of their data. No backup plan at all? Well, no data at all.

Other business only backup select systems.

#2 STICK TO YOUR BACKUP PLAN.

Create your plan and stick to it. You don't really have a plan if you only backup your data when you think of it (see the next page). The less frequently you backup data, the more likely you are to have missing data. That's even MORE likely if you don't check your backups (i.e., multiple backups failing or not completing).

We recommend a combination of weekly full backup and daily incremental backups for most businesses.

- For most smaller businesses, a full weekly backup is sufficient.
- You'll need daily incremental backups for regular work, client data, and businesses in regulated industries

There's a balancing act between frequency, cost, and business need; so explore all of your options to get the frequency that's right for your business.

#3 DON'T THINK. AUTOMATE.

Use the automatic scheduling feature in your backup software. As mentioned in the previous point, human memory is fallible—don't rely on it to protect your business' data.

We hear from clients and potential clients some variation of this every week: the servers went down, but no one was worried because they had a backup plan; then the IT guy sheepishly says, "I forgot to run the backup." Let the software do the work for you.

#4 PROTECT YOUR DATA.

This isn't exactly a backup point, but it's worth mentioning—invest in network security. Many small businesses don't think it can happen to them when it comes to security breaches. In addition to the damage to your reputation, there are also real costs to security breaches.

While most security breaches are targeted at stealing data; some viruses will simply destroy your information and data.

#5 INCLUDE ALL EMPLOYEE LOCATIONS.

Don't create backup for your headquarters and think you're done – unless every employee works there. As businesses become geographically dispersed—and employees can work from anywhere—plan to protect and backup data assets wherever they are.

Many employees will work at home on their laptop and do so offline. They might even use a personal service (Dropbox, Box, etc.) to save their work as a backup. You need to backup the information on laptops and PCs beyond the confines of company HQ.

If you're in a regulated industry, this goes double for you!

#6 DO NOT IGNORE MOBILE DEVICES.

There are more smart phones in the world than toothbrushes. Your employees are accessing emails, documents, and other work-related information on their phones and tablets (we hope they could also afford a toothbrush!).

You can't afford to ignore your employees' devices, so include them in your backup plan.

113 cell phones (that's 2 phones per second) are lost or stolen every minute—along with the gigabytes of data on those phones, and maybe the next brilliant business plan. Back them up.

#7 TEST YOUR DATA.

You don't want to think your back up is working, you need to know. As the saying goes, "Trust, but verify." Take the time to periodically test your backup system. Spot check to ensure a recently created document has been properly backed up. It's also a good idea to periodically test. Protect yourself.

#8 FREE TOOLS AREN'T A BACKUP STRATEGY.

Online services like Dropbox, Box, or Google Drive aren't backup strategies (at least when it comes to business). These are great places to store data, especially for personal use (and if you use them for business, PLEASE don't place confidential information on the free version of these tools). These tools aren't a plan, though they can be part of a plan.

#9 CHECK OUT THE CLOUD.

Cloud options for data backup are ubiquitous, secure, and cost-effective. By now, you should be over any lingering concerns about using the cloud for backup (or any other business need) because of security concerns.

The traditional tape and disk backup tools remain relevant as pieces of the backup puzzle for many companies. However, physical backups can be lost, destroyed, and they decay over time so need to be periodically refreshed (that means transferring data from old to a new piece of media). A disaster isn't required either. It's hot here in Vegas. If your AC breaks down, servers can easily overheat. Tape can break due to age, manufacturer defect, or mechanical failure.

#10 RAID STORAGE ISN'T BACKUP.

The "redundant" in redundant array of independent disks (RAID) doesn't mean you have a backup plan with RAID servers in house. There are multiple levels of RAID, so despite the "R" in the acronym storage might not be redundant. Plus, all of your data is still within a single stack in one location. RAID, depending on the version, can protect you from a single, or two, hard drive failures, but information could still be deleted by your users—whether accidentally or maliciously.

#11 DON'T FORGET COMPLIANCE.

Whether you backup in-house or outsource, the data is yours and it is your responsibility to ensure that you're in compliance with all relevant regulations particular to your industry. That means doing the research to ensure that your managed IT service partner is compliant with FINRA and other rules if you're in financial services, HIPAA if you're a healthcare provider, etc.

Outsourced and cloud-based backup systems can be compliant, but you need to be sure access control, auditing features, data encryption, and other security features meet your requirements.

#12 YOU STILL NEED AN ARCHIVE (MAYBE).

Your backup strategy is a key piece of long-term archiving but the two things aren't synonymous. Research and understand the regulations that dictate your industry's record-keeping requirements.

Information that must be kept for records management or archival needs will also be subject to more stringent retrieval and auditing requirements—such as legal holds in the event of ediscovery.

There's also a cost issue. You'll want to move long-term records that are infrequently accessed to less expensive storage options.

#13 ESTABLISH RECOVERY OBJECTIVES.

Determine both your recovery time objective (RTO) and recovery point objective. Your RTO is a measure of how soon you need to be back up and running after a failure. The recovery point objective (RPO) is a measure of how much time data can be lost and not how much data will be lost in a certain period of time. So if a business can only lose 15 minutes of data then their RPO is 15 minutes

#14 GEOGRAPHIC DISPERSAL.

Keeping your backup tapes in the server room across from the servers they just backed up eliminates the possibility of recovery in the case of fire, flood, or theft. Likewise, having your IT guy bring backup tapes home to have "offsite storage" is a misplaced step in the right direction.

Keep information in at least two locations. A built-in advantage of a cloud backup service or other outsourced service is geographic dispersal. Your data will be on your hardware as well as with your service provider—and backup services providers have their systems geographically dispersed for backup and disaster recovery.

Have your backup data (physical or electronic) in different locations. That doesn't mean a different room or floor in the same building—find another building! And another building on a different power grid is even better.

CLICK HERE TO SHARE →

ABOUT AIS

Our purpose is to provide superior quality multifunction copier, printer, fax, and software products and managed IT services to businesses and organizations in Southern Nevada and Southern California. We believe that for each customer we service, performance of our products and staff is what makes the difference.

As a locally-owned independent dealer, we have the flexibility to create or select from a variety of resources, so that we use only the very best programs to fit each customer's individual needs. Our mission as a Company is to exceed our customers' expectation by providing unparalleled business solutions with leading-edge technology products, coupled with unmatched service, supplies, and support. Our foundation of work ethic, integrity, and teamwork enables us to work within a culture that cares about our customers, our community, and each other.

NOW THAT YOU UNDERSTAND WHAT YOU NEED TO BE THINKING ABOUT WHEN IT COMES TO DATA BACKUP, THINK ABOUT THIS:

Do you have the time to figure all of this out yourself?

Isn't it time to let the experts manage your IT?

CLICK HERE
to schedule a no-obligation conversation with us to discuss if managed IT services is right for you.

Contact us today to get the help you need.

ONE COMPANY, MANY SOLUTIONS

Monique Phalen is AIS' Director of Technology where she is focused on building better business outcomes for clients. She enjoys putting the technology puzzle pieces together for clients so that they can focus on their business, not their IT infrastructure.