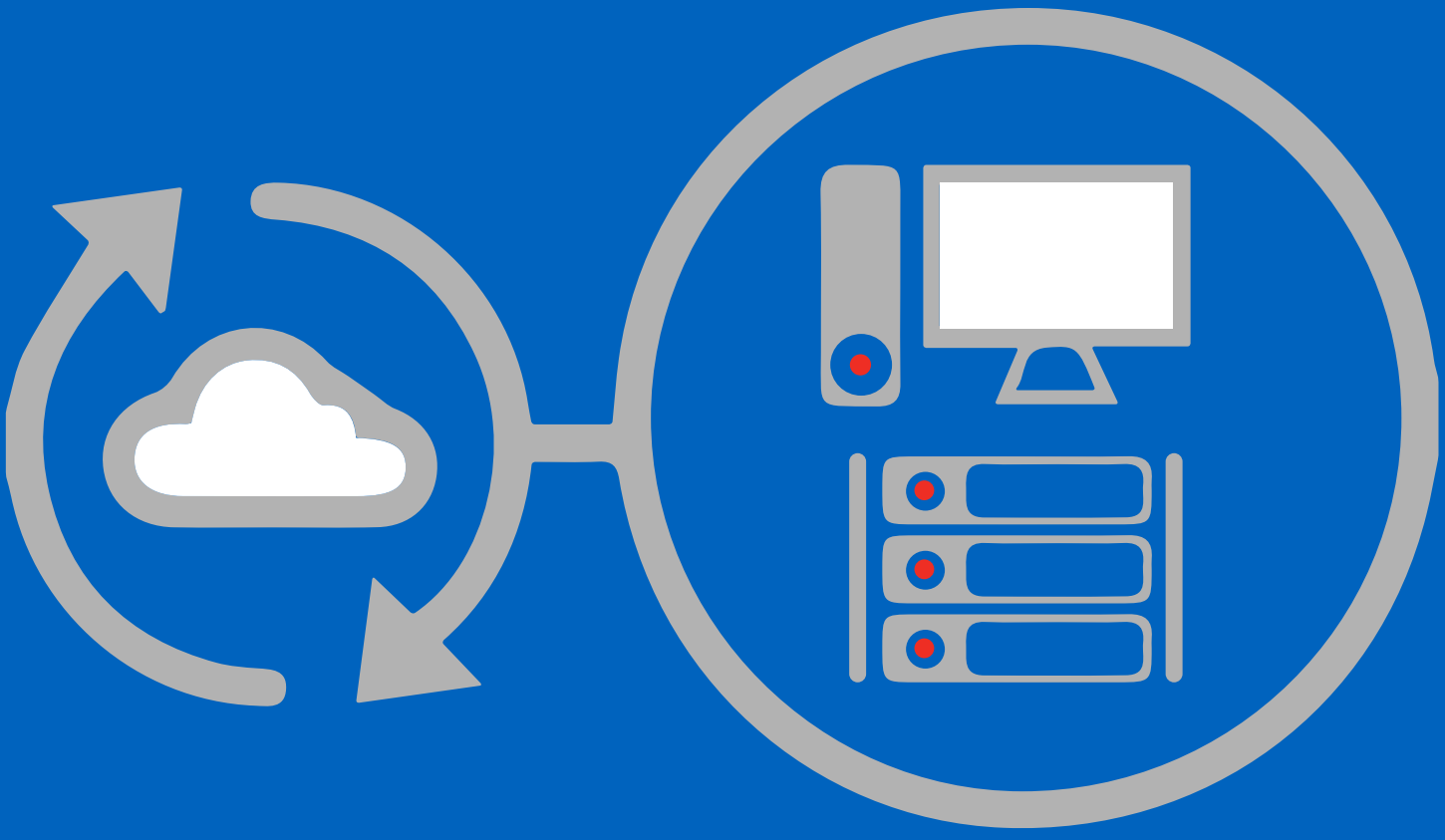
All Covered
IT SERVICES FROM KONICA MINOLTA

ABS

PROTECTING YOUR MOST PRECIOUS DATA



Regardless if you are an IT professional or not, we all understand the importance of backing up and protecting your most precious data on a regular basis to some type of external media or cloud-based system. Just about every industry today relies on computers to complete daily tasks. We have all experienced an accidental hit of the delete key at least once after hours of laborious work. That quick hit of delete would be followed by a panicked phone call to the IT department to see if there is a way to get the lost file back.

The example above is obviously a smaller-level issue (even though it may feel huge for the user); however, the topic of server backup procedures is often a much larger consideration for businesses today, which also requires at least a rudimentary understanding by end-users as well as all IT staff. For example, many users “save” their files on their desktop, not realizing it is only their local hard drive. This ultimately means these files are not generally part of IT’s backup process. If something happens to these files, the end-user will really have a problem, as they have not been replicated anywhere at all.

Additionally, there are more and more regulations associated with keeping data backups in a particular format, such as the GLBA, SOX and the HIPAA Security Final Rule in the healthcare industry, which can add to the complexity and requirements managed by IT. This is why it is increasingly important to have a complete and well-documented server backup plan.

Backup Scenarios

CONSIDERATIONS

There are many different reasons why server backup plans are important. There are a variety of different situations that can take place within a server room and the IT team must have a well-documented procedures so they are ready to act at a moment's notice. Hardware failures comprise more than one-half of disasters for small to mid-sized businesses, according to the Quorum Disaster Recovery Report, Q1 2013 and it takes an average of 30 hours for recovery.

Hardware failures comprise more than one-half of disasters for small to mid-sized businesses, according to the Quorum Disaster Recovery Report, Q1 2013 and it takes an average of 30 hours for recovery.

DISASTER RECOVERY

IT has made great strides in the last decade when it comes to backup options. Today, solutions are far more sophisticated than just a decade ago thanks to technologies like cloud storage. At best, companies ran a backup of a server over the weekend and the tapes would go off-site to a storage facility. The backup process may have been taking place, but not much consideration was given to the recovery process. It wasn't until IT professionals were asked by colleagues to pull files from those backups that they really thought how to capably recover those files. IT had to re-think their server and data backup plans to include how to get back online efficiently and not just focus on the backup process. According to the National Archives & Records Admin in Washington, 93 percent of companies that lost their server room for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster.

HARDWARE FAILURE

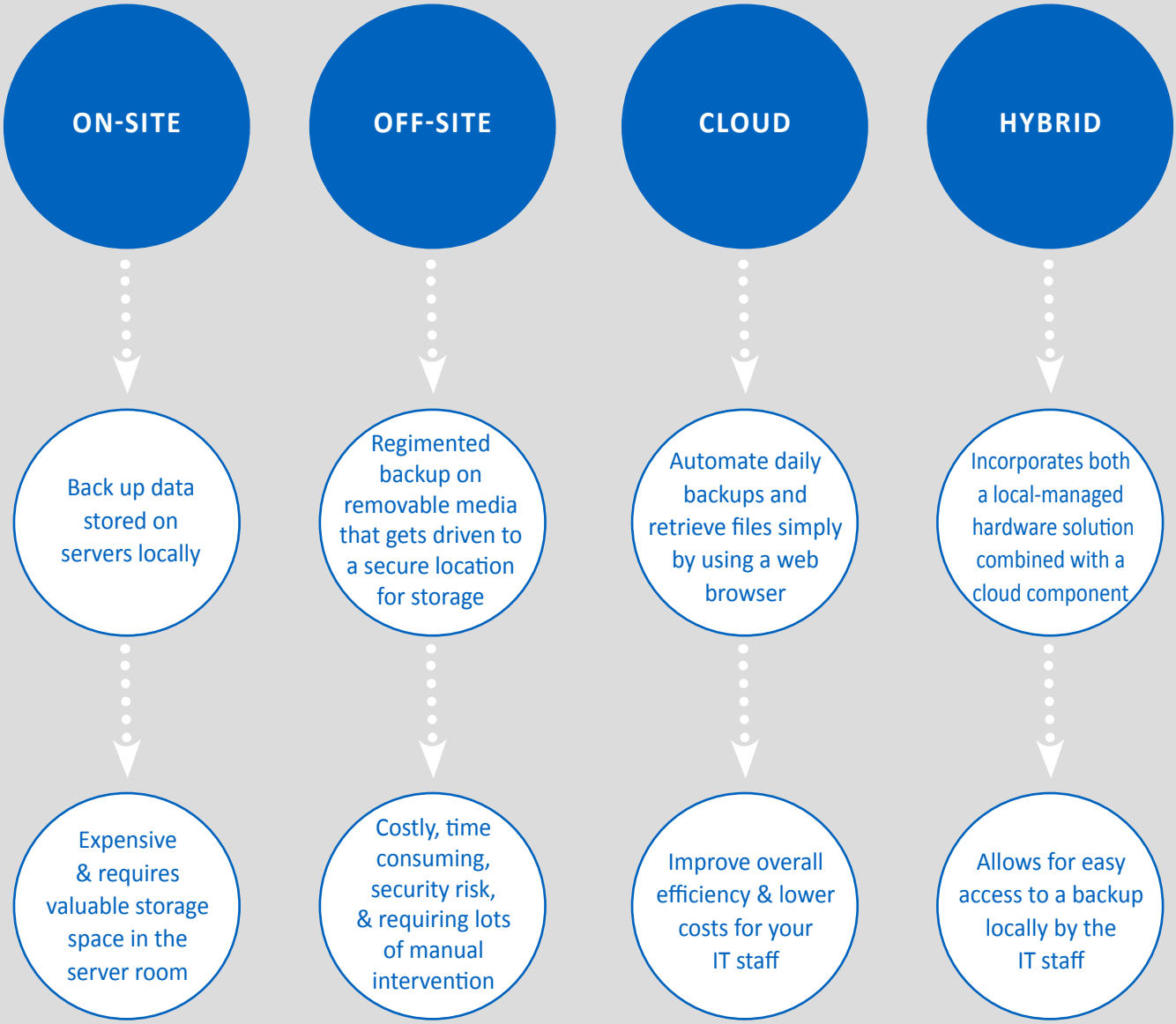
The thought of a hardware failure in a server room or data center can send shivers down the spine of any IT professional. While no one wants to think about it, IT professionals are constantly considering how to manage "worst case scenario" circumstances and the best ways to bounce back from them. A hardware failure can end up as a costly, stressful, and time-consuming situation to manage. Although hard drive manufacturers claim a less than a one percent failure rate, computer scientists at Carnegie Mellon University found that a two percent to four percent failure rate is more commonplace. In some instances the failure rate may reach as high as 13 percent.

LEGAL AND REGULATORY COMPLIANCE

Is your business involved in the healthcare industry? What about stock trades or financial planning? Many industries such as these have specific requirements regarding what data needs to be backed up, how often, who has access to those backups, and so on. It is important that IT administrators understand, and comply with, all the industry requirements and regulations related to data backup, and more importantly, can prove they are following all required procedures in case of an audit.

On-site, Off-site, Cloud – Which is Best?

In the last few years server backup best practices have undergone an amazing transformation. What was once considered standard operating procedures are now considered antiquated and risky to the core of any business. As a result, IT teams have had to re-think their entire backup plan.



ON-SITE

Historically, the IT team would back up data stored on servers locally to tape systems or other similar media and then keep it on hand in case it is needed. Even though tapes are an older technology, they are still widely used and have a place in many IT departments, keeping their high level of importance in backup and data recovery processes. While convenient for the team, it can prove to be quite expensive as well as require valuable storage space within the server room. Additionally, storing backups on-site can leave it vulnerable to damage if there is some type of natural or other disaster (such as a flood or fire). While some businesses still use strictly on-site backups, it is generally considered risky.

OFF-SITE

An off-site backup typically consists of a regimented backup on to tapes, disks, or other removable media that would get picked up and driven to a secure location for storage. This shuttling back and forth of data would normally take place at least once a week through a data security vendor. If a restore was required, a member of the IT department would contact the vendor, request a return of the tape (or other media) back on site to complete the request. A standard turn-around would usually be 24 to 48 hours to get the backup back on site and then another 12 to 24 hours to retrieve the file. While this backup strategy helped to protect against potential on-site catastrophes, it was, however, quite costly and time consuming, as well as requiring lots of manual intervention.
Off-site media backups can also be a security risk, as the media could easily be lost or stolen. It is also important to remember a tape backup does not guarantee you will recover the data, which is why reviewing backup logs and testing tape restoration is so important.

CLOUD

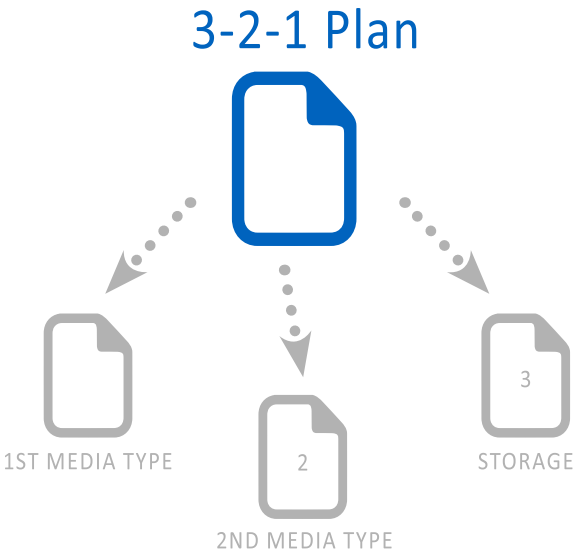
A cloud-based solution for backup is increasingly popular for a variety of reasons. You can easily automate daily backups and retrieve files simply by using a web browser. This can improve overall efficiency and lower costs for your IT staff. A key part of a cloud-based backup process is that an adequate amount of bandwidth is available to efficiently complete a backup and restore process. Some businesses find a cloud backup solution particularly attractive if they are already using a cloud-based system for their server storage. If their data is already stored in the cloud and there is buy-in from non-IT management regarding its reliability, it is an easy choice. Cloud-based storage is also becoming a more viable option for SMBs as Internet bandwidth continues to decrease in cost and improve in speed.

HYBRID

One option that is gaining popularity is developing a hybrid backup option, which incorporates both a local-managed hardware solution combined with a cloud component. This solution allows for easy access to a backup locally by the IT staff, however, if an issue arises and the local backup is in accessible for some reason, the cloud backup can be easily accessed, providing an added level of comfort– sort of a backup to the backup…

REDUNDANCY: A BACKUP TO THE BACKUP

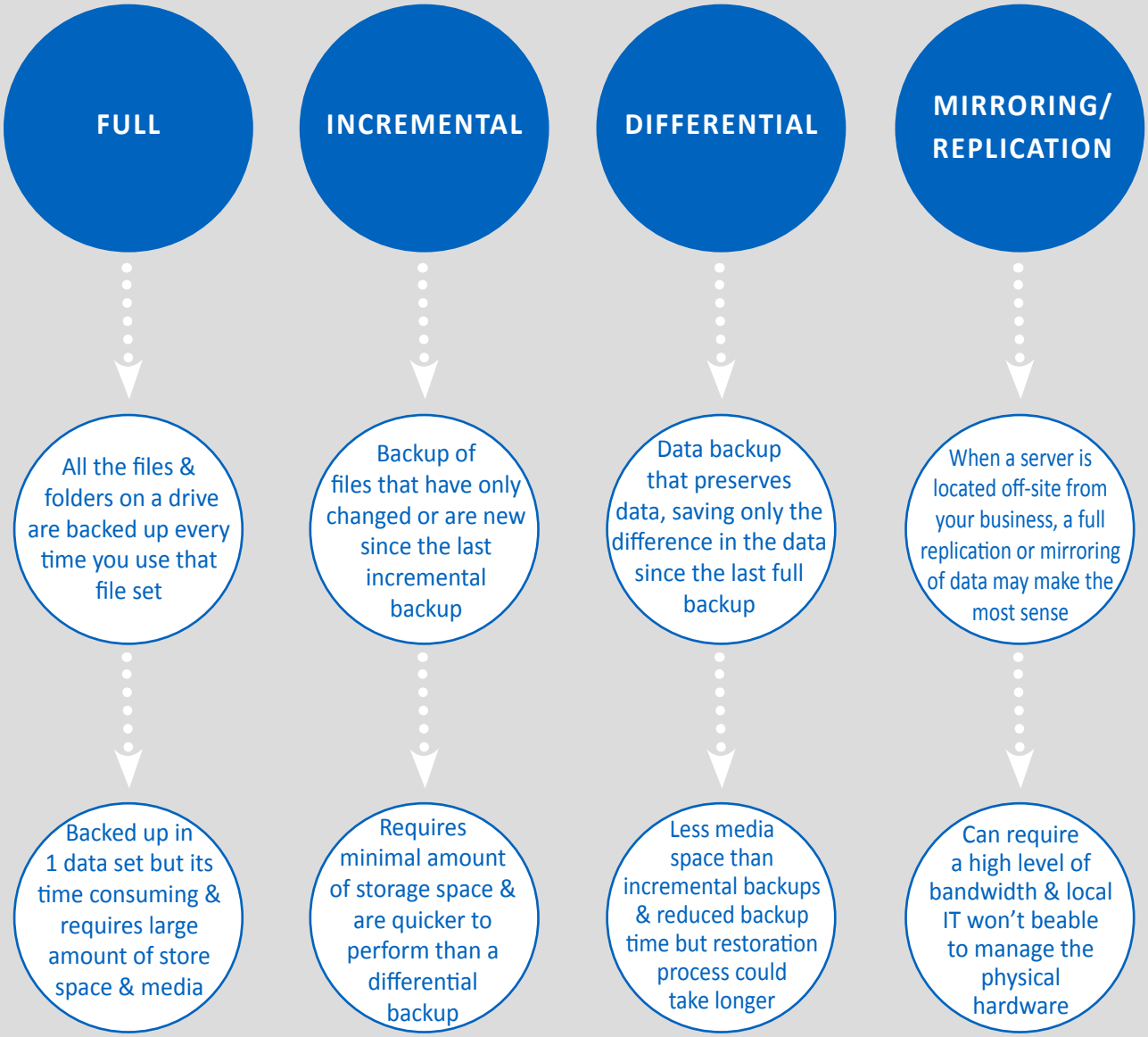
It is the job of IT to think of all the different scenarios that could happen to a company's computer and server systems and develop procedures to protect them from disasters. As mentioned previously, IT professionals base their entire career on preparing for the "worst case scenario," and having a backup to the backup just makes sense. A redundant backup process can include a combination of on-site and off-site, or incorporate a backup protocol in the cloud. By having a combination solution, IT will be able to retrieve files easier. More importantly, IT will be able to get servers back online quickly and efficiently. It will also improve the possibility of retrieving a file without issue. For example, if for some reason the physical tape kept on-site fails, the IT team can quickly take advantage of the backup in the cloud. According to Gartner Technology Research, 50 percent of all tape backups fail to restore. If that one tape was your only backup for that file, database, or other key piece of information, you will start praying to the server gods quite quickly to make it work.



Many IT professionals follow what is referred to as the "3-2-1 plan." Three copies of any file deemed important enough to backup. Use two different media types for your backups. One of your backups should go off-site for storage.

Backup Types

Just as there are many different ways to approach the storage of a server backup, there are just as many ways to run a backup. Each backup type has positives and negatives which will require consideration based on the individual business as well as any industry requirements.



FULL

A full backup is exactly as it sounds. All the files and folders on a drive are backed up every time you use that file set. The IT staff simply selects the files, drive, etc. to back up and the destination where the files should be backed up and the system will backup everything in that specific location. In this scenario, all selected information is backed up in one data set and if a restore is required, only the single backup data set is needed. Full backups, however, are quite time consuming and require a copious amount of store space and media.

INCREMENTAL

An incremental backup provides a backup of files that have only changed or are new since the last incremental backup. If (or when) a full recovery is needed, the recovery procedure would require the last full backup in addition to all the incremental backups until the point-in-time of the needed recovery. Incremental backups require a minimal amount of storage space and are quicker to perform than a differential backup. The purpose of an incremental backup is to preserve and protect data by creating copies based on only the differences, which reduces the total amount of time needed to perform the backup.

For the first incremental backup the process includes:

- Backing up all files, just like during a full backup
- During the next backup only the files that have changed or are new are backed up
- If you use the same file set again, only the files that have changed (or are new) since the second backup are backed up
- This logic continues each time a file is changed or a new file is created

DIFFERENTIAL

A differential backup is a type of data backup that preserves data, saving only the difference in the data since the last full backup. As opposed to an incremental backup, only two backup media are needed to restore all the requested data. When a full backup and a differential backup are combined all the files, changed and unchanged, are recovered.

Generally, differential backups request less media space than incremental backups and the time involved to complete the backup is greatly reduced. It is important to note, however, while this can streamline restore requests for IT, the actual restoration process could take longer as you may need to restore both the differential backup and the full backup. Additionally, recovering a specific file will require IT to locate the file and determine whether it is on the differential backup or the full backup.

MIRRORING

When a server is located off-site from your business and is often owned by a third party, a full replication or mirroring of data may make the most sense. The local IT team can manage the server as if it was local in their data center or server room.

It is important to remember that mirroring can require a high level of bandwidth depending on the amount of data in the backup. Additionally, local IT will not have the ability to manage the physical hardware where the server is located. As long the bandwidth is available, a complete restoration of data is often quicker than the other types of common backup practices.

Just like in physical backup scenarios, it is critical to have duplicated backups in various locations. The backup process is more than just "backing up data." The backup and recovery processes need to be considered as one procedure and should be reviewed regularly.

WHEN SHOULD BACKUPS RUN?

The answer to this question will vary on multiple factors. Historically, IT would set a backup to run over a weekend, overnight, or some extended off-hour time period when no one was generally at work. Now, thanks to laptops, VPN connections, and more and more employees working at home or from the road, the concept of "server downtime" no longer exists. As a general rule, however, backups are still usually run on the weekends or during off-hours due to decreased activity as opposed to the work week. Additionally, backups can take anywhere from several hours to a complete day, depending on the amount of data scheduled for the backup and the type of backup scheduled. For example, a full backup could take an entire weekend while a differential or incremental will take far less time.

It is important to remember that backup archives should rotate through a variety of archives instead of repeatedly overwriting the same file continuously. If the file becomes damaged or corrupted, you still have a previous successful version on hand just like multiple backups.

What Should Get Backed Up?

Just like the question of "how often should backups run," the question of "what should get backed up" is just as varied. A successful backup procedure begins with selecting groupings of data. Deciding what to back up and when may sound like a seemingly simple question, however it is not. For example, if too much redundant data is backed up, the data store will fill up quickly and take a long time to complete. By backing up too little data, information and files are easily lost. It is also important to determine what should be part of a formal backup and what should be part of an archive. For example, if a file is completed and should be kept for historical purposes or will not require constant access and adjustment; that should be part of an archive. If a file will require constant access and updating, it should be part of a backup plan. It is not uncommon for files related to a specific project have a backup procedure; then once the project is complete, it is moved to an archive.

When deciding on what should get backed up, some considerations should include:

- How important is the data on your severs?
- How critical is that data to day-to-day business?
- How often does the data change?
- If a restore is required, how quickly does the data need to be available again?
- Do you have the equipment to perform backups? If not, are you ready to make the capital investment?
- Who will be responsible for the backup and recovery plan?
- What are acceptable recovery time objectives (RTO) based on different failure scenarios?
- What is the best time to schedule backups?
- Where will you store your backups?
- Are there any guidelines or regulations that will dictate what you need to backup?

FILES/FOLDERS

Files and folders are generally considered "active data" as they are constantly changing. Dependent upon the type of information contained within those files and folders, the potential loss of that information could prove catastrophic. While the initial urge will be to back up "everything," in reality, that may not be necessary.

Files related to personnel, tax records, financial data, and information for regulatory compliance should always be at the top of the list when deciding what data should get backed up. Additionally, this is the type of data set that should be a part of multiple backups, as well as within an off-site backup.

DATABASES

Databases are also often considered ever-changing and critical data for a business. Dependent on the type of database, it is a good idea to back up the physical database files. Ultimately, however, the final decision on how to back up, as well as a retrieve, a database will greatly depend on the type of database involved. A SQL database may have a very different procedure than an Oracle database.

EXCHANGE SERVER AND EMAIL

IT and end-users alike understand the importance of backing up email (often using Exchange). Exchange servers should get backed up regularly to ensure all mailboxes and system-related data can be recovered in the event of a crash.

Exchange is often considered one of the more complex backup procedures due to everyone's constant use of email. There are a variety of different protocols available and the final procedure will have a lot to do with company size, Exchange server size, and version of Exchange in use. For example, Microsoft offers backup applications as well Microsoft Exchange server 2010 plug-in for Windows Server Backup. Many third-party vendors can also provide customized backup procedures. Another option is using cloud archiving for email in a similar fashion as using cloud storage for standard data backups. Third party organizations, such as Intermedia, can provide email storage as an add-on service for a variety of different platforms, such as IBM Notes, GroupWise, and Exchange.

WHAT ABOUT APPLICATIONS?

The term "application" can mean different things depending on your job function. Are you using Microsoft Office or managing a website? Each example utilizes the term "application," however, the ramifications of these two examples going down are vastly different. Identify which ones are desktop-based applications and which are system applications that are necessary to keep a business online. If an application isn't deemed "backup worthy," think about the preference files and see if they should get backed up.

Recovery & Restoration Plans

It is obvious that the backup plan is important and should be well thought out. However, many do not think about what should happen when a recovery is required; especially in a catastrophic situation when entire servers require restoration. In reality, the backup process and the recovery process need to be developed as an entire procedure.

DOCUMENTATION

Documenting processes and procedures in IT (not just backup and recovery) is incredibly important, however, it doesn't happen nearly as often as it should. The "what if you get hit by a bus" is often jokingly said, but never acted upon. What is far more realistic is someone is away on vacation, dealing with a family emergency, etc. and someone must stand in. If processes are not properly documented, it will not just take additional time to get back online, it runs the risk of potentially damaging the backup during the recovery process, or any other IT process for that matter. This should include what happens if there is a hardware failure as well as a data loss. If everything is backed up to a tape, what is involved with potentially "building" new server? Is there more of a Band-Aid option that can be put in place until the original hardware is repaired? This is one reason why hybrid-based systems are becoming popular, as the hardware is in two different locations. If the local server backup fails, the cloud storage is quickly available.

STORAGE CONSIDERATIONS

Employees often look at server storage like a bottomless pit. They just add more and more data to it without any worry that at some point it may require off-loading and storage of older data. In reality, a server is much more like a file cabinet. From time to time, it will require purging. There is a limit to how much it can store at one time and the IT team should have well-documented (as well as well-communicated) live storage limits and procedures for employees to request the recovery of older data.

LOGS

Logs for a backup procedure go far beyond a simple documented list. Backup logs can include how long the backup took to complete, if any errors occurred, the number of media involved, and so on. This information may sound somewhat dry, but to a server administrator, this is critical data to help stay informed on the health of the backup process as well as identify any potential reoccurring issues that require attention.

When it comes to SQL Servers, the databases utilize a full or bulk-logged recovery model. At minimum, one full backup must be completed before you can create any log backups. Once complete, the transaction log can be backed up at any time unless the log is already being backed up. Typically, a database administrator will create a full database backup on a periodic basis, such as weekly, and then will create a series of differential database backups on a daily basis. Transaction log backups will run even more frequently, such as every 10 minutes. This scenario can vary depending on the type of data stored in the database and how often the data is accessed or changed.

PROCESS REVIEW/CHANGE MANAGEMENT

Any time a change in procedure associated with a backup or recovery process is required, it should be a team review within IT. These important procedures require a well thought out plan. The new procedure needs to be detailed in a use case and then tested in tandem with a standard backup. After the backup (or recovery) test is complete the results should be compared to the current plan to make sure the change does not negatively affect the outcome of the backup or recovery. Once a decision is made, the procedure should be well documented and communicated to the entire IT team.

HARDWARE BACKUP

Just as it is important to be ready with a data-based backup solution, IT needs to be ready with a hardware-based backup. If a main server fails, what do you do? Yes, you thankfully have everything on tape, but what is required to get everything needed off that tape and functional again? While the IT team is documenting the complete recovery process, the hardware recovery process should be included as well. In reality, a complete “blank” server should always be ready to go with the ability to run the most business-essential files until the complete serer is back up and running. This can be an incredibly expensive proposition, which is again why more and more companies are looking at a hybrid option that includes some type of cloud-based storage.

In Conclusion

Backups are obviously an incredibly important part of any IT infrastructure as well as day-to-day business activities. They require a comprehensive plan that identifies all key aspects of a business, adheres to any regulatory requirements and is well documented. Most importantly, the entire plan as well as the backup and recovery processes should get tested and reviewed periodically. The role of IT is ever-changing and it is critical that the IT team stays up to date on best practices and is always ready to handle that "worst case scenario."

About All Covered

All Covered has been providing individualized IT consulting since 1997. A division of Konica Minolta, All Covered focuses on meeting the unique needs of every business by developing customized IT solutions for networks, including:

- Computer and Network Consulting
- Planning
- Design
- Procurement
- Implementation
- Maintenance
- Management

All Covered can guide any business through the rough waters of IT management and successfully supports organizations across America in just about every industry. While a national company, All Covered has local offices so experts are always available to support any type of business.

Let us help you with your server backups.

Contact All Covered toll-free at 866-446-1133 or visit www.allcovered.com.