What You Must Know To Protect Your Business And What They Aren't Telling You

Whitepaper For Small Business Backup & Restore

Table Of Contents

Intro

We know we need backups. We know we should be doing them but few of us are certain we have reliable, restorable backups with all our critical data. I've been in this industry a long time and know first hand how system failures strike out of the blue, completely unguarded and I've seen the devastating and business crippling effects it has. Learn how to check your backups and if they are fully restorable. In this white paper we'll go through the risks, what to backup, the common failure points, what your backup should be doing and some other tips and tricks with the goal to ultimately keep your business up and running?

This could be the most important read of your year.

Why Backup?

Most people answer they don't want to recreate what was done. Ignoring the cost factor of not only having staff reproduce what was lost coupled with the factor they are pulled away from their primary job of actually making you money. The fact is most things can't be recreated. We don't remember what was written. There is too much information we keep in this day and age.

More importantly some of the data is there to protect you. Emails that had given you approvals, scans of signed documents, pictures used as proof and documentation - you can't recreate that

In some professions you may be liable without proof, the proof in those images, emails and other files! So you want to **make sure you have backups to protect yourself from liability, loss, business continuity and professional image**. Blaming computers use to work in the '90s but now your customers and clients are savvy enough to know there are systems you should have in place to protect their info and your business.

In addition to the inability to restore data is the consideration for the **time it takes to get back up and running**. When (not if) your computer/server dies there is a considerable amount of time just to get either it up and running or a new one.

As a business owner you need to be able to answer the question "How Long Can I be down?" and then have a recovery plan to suit that requirement.

Bear in mind while your systems are down your still paying your staff (how long before you send them home?) you can't get your work done which ultimately means your not generating income. So how long can you afford to be down?

Data loss occurs for all kinds of reasons. They fit in two categories. Hardware or software failure. The best case scenario is only software needs to be reloaded. This, on average, takes

up to 8 hours. Sure you can load an operating system in as little as 20 minutes but you are being highly misinformed if you believe that. Here's why, by the time you find the installation DVD...oh wait your system didn't come with one, you'll have to download. That's half hour to find the link to download, now you need a thumb drive to save to plus a "How to Save an OS To Be Bootable From A Thumbdrive" set of instructions, but wait the drive has files on it so you need to copy those off first. After that's done your informed the drive is too small. Scramble through the office...go to the store...finally get a drive. Now it takes 20 minutes to do the install. Then run the updates which takes hours. Then load the software like office (need to find the install dvd for that...oh wait you downloaded it and the software keys were left in email...which is now gone). If it's newer you could log into your microsoft account...if only you could remember your username and password which was saved but gone now. This is how reinstalls happen day in and day out. They are a pain and I paint it this way to encourage you to take the proper steps NOW to prepare for that day when you lose data. It's a lot less pain but you have to take steps now!

If the hardware is an issue like a bad hard drive or motherboard then we need to add on the time to get parts shipped in or a new system. If the motherboard is gone and we can't find a like model we will have to do the software reinstall as well...plus the physical installation.

So now that we know why we should back up let's move on to what things we should backup and what are the most missed items.

What Should Be Backed Up?

The answer to this question is best known by you, for the most part. You'll know which files are most important. Which ones you absolutely must have and those that would be nice to have. You might not know where they are stored but you know the "books" need to be backed up, all your client info, images and databases. What you might not know is that many databases can't just be copied. The database itself must be stopped and a special tool is needed to backup the database. Many bookkeeping programs don't store the books in with your users documents but rather in their own special location. The same applies to many other programs that store in their own specific location making it difficult if not impossible to do one specific backup. Emails are often forgotten in backups and many of the email programs need to be exited before a proper backup can occur. Settings for programs should also be backed up if possible. For example do you know your email password and server settings? Do you have profiles saved? If your doing it manually do a search on youtube for backing up outlook (if that's your emial program)

Use this Cheat Sheet to Help You Build a List of Backup Items

Computer Name:_____

Name of Program	Location of Saved Files	Is it a database	If database: Do I need a backup tool	Do I have settings/profile in the program that needs backup

Once you've done your list this will cover the basics of your backup strategy to protect your business.

One of the other things to consider when backing up is a complete image of your systems. This will help in the event of a major system failure and will get you back up and running quickly. We will talk more about this later. The important thing is we have your key business data backed up.

How Do We Backup?
There are a few prongs to this questions. One is "what are we physically backing up too" and the other is "how are we accomplishing those backups". These two prongs work in conjunction to eliminate risks.

What Hardware Should Small Business Be Using To Backup
Let's deal with the hardware first. Many people backup important files to zip/thumb drives. Those little drives that plug directly into the computer. The problem with those is that they tend

to fail without warning. You plug them in and they simply cannot be accessed. They get lost or misplaced easily. Staff write over them when they need something quick to save too. They also need to be safely ejected which is often not done. **This corrupts the backup and renders it useless.** They are often left plugged into the computer and are **prone to virus attack and power surges which often render them useless.** They need staff intervention which introduced human error...the most common error of all.

Some people still burn DVD's or use tapes. Essentially the same problems plague these devices as well as the addition of speed issues to do a backup and restore. Tapes have the additional problem of needing to be swapped out and they seem to have a poor track record with many not being able to retrieve data when the tapes age past a year old.

Some people will opt for the online backup which keeps all your data offsite and that's good but buyer beware. Your data is no longer on your equipment. One of the biggest caveats you must know and no one mentions this, is the **amount of time it takes to restore your data**. I have seen companies take weeks to get back to business because the online restore took that long. Many times you'll wait all day for a restore only to find out at the end of the day there was a hiccup and the transfer didn't complete and you have to start all over again.

"One of the best systems to use is a dedicated backup system"

These devices sit on their own and are dedicated to one job - protecting your data. These use their own hi speed drives so restores happen as fast as possible. A good system should have both onsite and offsite capabilities. This gives you the best of both worlds. **Fast, automated and restorable data** as well as the security of offsite in the event of major catastrophes. Dedicated Backup Systems!

Other risks would include power surges and electrical grid issues. **Your dedicated backup system should be plugged into a good Uninterrupted power supply (UPS)**. We had one client who lost their server when a truck drove into the power pole a block from their office. These things happen.

Backup should also be kept in a secure location. The obvious is to protect from thieves but also from disgruntled employees who seek revenge on your business, accidental issues such as items falling into the backup device. We've seen drinks spilled and ladders knocked over onto equipment. So lock up that equipment. It's there to protect you and you need to protect it.

Now that the hardware is handled we can move onto the software.

What Software Should I Use For Backups? There are literally hundreds of backup software choices. These are the features you must have.

The software should be:

Automated: Silently working in the background doing it's job day in and day out. Your staff should NOT have anything to do with it! When people get involved mistakes happen. Remove the human element

Self Checking: The software should check itself for errors and make sure it has done the backups correctly. Only then should it alert one of the humans if something is wrong.

Multiple Copies: The software should keep multiple copies of backups. This will allow you to go back a day, a week, months or years. I've seen this help on a large scale when a virus wiped out several directories but wasn't noticed for a few days. A normal backup would have overwritten the last good copy with the virus. A multiple version allows you to go back many versions and days. I have also seen it work when a staff member edited a rarely used but important document and the mistake wasn't noticed for months later. On many systems you can only go back to the last backup but a properly configured backup system should allow you to go back many months, years or a set number of versions.

Strong Encryption: The software should be encrypted. Imagine if your backup falls in the hands of hackers or thieves. You wouldn't be the first business threatened with the turn over of personal client data unless you paid a ransom or have client lists & sensitive company data sold off to competitors. Even nosey staff have been known to explore the backups as an easy way to access files that are normally locked on the server.

Virus and Now Cryptovirus/Ransomware Protected: The software should be immune to viruses. The latest attack on companies is crypto viruses which essentially locks your files and backups and demands a ransom before they unlock them. We have developed the world's first and fastest crypto virus protected system which protects your from these threats. Through a series of safeguards, checks and balances we have provided a system that will protect your backups from crypto viruses and ransomware.

Restore Speed: Time is money. How long can you afford to wait for backups to restore? Hours? Days? Weeks? Expenses keep rolling in even when you're down and that's why you can't afford a slow restore time. Let alone keeping the customer waiting while backups restore their information. The problem with many online backup solutions is the time it takes to restore the data. You are at the mercy of the backups internet connection speed, your connection speed and the quality of the connection. Too many times we have seen what should be 8hr transfers turn into days and weeks because after the 8 hours it shows a bad download failure. Off site is ideal for small amounts of data and for security against onsite hardware destruction from things such as floods, thefts, and fire. However for true security you should have a hybrid system that combines both onsite and offsite.

This is the basis for backup. It will allow you access & retrieval of your files and data and is the fastest method to backup.

System Image

Previously mentioned was performing a system image. A system image is basically a mirror of your system. We take this image of your system when it is good and healthy. We save that image on another hard drive. When catastrophe strikes we can literally plug that drive directly in and instead of 8 hours plus of setup your back up running (to the point in time the backup was taken) within as little as 10 minutes. For the extra files we saved after that point we then access them from our file backup. For example on Jan 1st you decide to initiate a backup plan. Your current systems are healthy and we take an image of them. We then also setup a file backup that regularly backs up your files. Just over two months later, on Mar 15th, your hard drive crashes. We simply plug the system image drive into your computer which takes about 10 minutes and gets the system up and running with all the data up to Jan 1st (the date of the systems image) for the remaining files from Jan 2nd to Mar 15th we do a restore of those files from the backup server. The time it takes will depend on the amount of data to restore.

Some people ask if they need a seperate hard drive (between $80-$150 on average) for each of their computers? Only if you want the very quickest recovery time. An alternative is to purchase one large drive and save the images of each of your systems onto that one drive. You should then make a backup of that drive as well. When a system fails you boot into a copy tool that restores the image back onto that system. This usually takes between 20 minutes to just over an hour.

Another solution is to have all the systems work as virtual machines however it slows performance down and adds several layers of complexity.

What You Need To Know For The Future

You need to test your backups. Do a restore and make sure your files are restorable. That's the acid test. It's work & time but it's worth it. When adding new software or making changes make sure it the new software and changes are added to your backup plan. With this information you will be well protected and guarded against data loss.

When it comes to backups there is no one solution works best for every business. You should talk with a backup specialist about your needs so they may create a plan that works best for you & your business.

At Systems 10 we have created the world's fastest crypto virus protected and most secure backup system. If you would like to know how to protect your systems please contact us at backup@systems10.com or at http://systems10.com/contact

12 Most Common Reasons Backups Fail

1. No Backup Or Current Backup - most seen with companies requiring staff to plug external drives in for backup. Staff forget or put off the backup in their rush out the door.

2. Wrong Or Only Partial Data Backed Up - quite common. On first setup most businesses have an 80% chance of having all the correct info backed up. Often missing important things like emails, database dependent files, Financials stored in seperate locations. Overtime as new software is updated, changed and added backups need to be aware of those changes. When was the last time you had your backup analyzed?

3. Failed Backups - have you ever tested your backup? Is the backup recoverable? Too many times we have come across backup media that failed to copy the backup

4. Only One Copy Of Backups - redundancy is the name of the game. Don't trust your backups to one type of media or one hard drive. You should have backups on multiple devices at multiple locations

5. Backup Kept Onsite - Keep backups both onsite and offsite for maximum safety and ease of restore.

6. Unsecured Backups - We use the same encryption the banks use keeping your files private

7. Backups Left Plugged In - extreme power surges or virus attacks can wreck any connected backup device rendering your backup useless

8. Not Automated - human error is the greatest cause of failure.. Backups should be completely automated. Eliminates the risk and frees up your staff

9. Backups Not Protected From Cyrpto Viruses - there is a new attack that is extremely dangerous to business; the crypto viruses. Locking all important files and leaving a ransom note on your computer demanding payment. Many have not got their files back even after paying. Some of the infections wait for backup drives to be plugged in before dropping their payload infecting the backup first then the computer so you can't restore. We have developed the world's first crypto protected backup program which protects you from this and other attacks.

10. Equipment Failure - one in 4 drives will die a year. Servers will quit and backup drives fail

11. Power Issues - we had a client who lost their systems due to a truck hitting a power pole down the street, plus lighting, power surges, brown outs

12. Employees - either accidentally unplugging drives unsafely, forgetting to do backups, the revenge/disgruntled employee

Facts:

1 in 4 hard drives fail per year

Companies with less than 1,000 employees that experienced a ransomware attack had to stop business operations immediately - Osterman Research

On Average Small companies lost over $100,000 per ransomware incident due to downtime. One in six organizations endured 25 hours or more of downtime.

Can be liable - in 2013 Adobe was fined 1 million for a data breach

Data loss is up 400% since 2012, while 71% of organisations are still not fully confident in their ability to recover after a disruption.

Only 6% of businesses have a plan for disaster recovery

31% of all PC Users have lost all of their files due to events beyond their control

60% of companies that lose their data will shut down within 6 months of the disaster

93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster. 50% of businesses that found themselves without data management for this same time period filed for bankruptcy immediately. (National Archives & Records Administration in Washington)

Companies that aren't able to resume operations within ten days (of a disaster hit) are not likely to survive. (Strategic Research Institute)

Simple drive recovery can cost upwards of $7,500 and success is not guaranteed

Hardware failure is the leading cause of downtime (45%)

Unplanned downtime losses include lost revenue, lost productivity, recovery expenses, equipment replacement and more. Industry experts calculate between $926 and $17,244 per minute

In 2016, Marin Healthcare District was hit with ransomware & was unable to access patient data for more than a week & they lost 2 weeks of data because their backup systems failed. 5,000 patient data records were lost. This could have been avoided with properly tested backups

2017 Cockrell Hill Police Department in Texas was also hit with ransomware and lost 8 years worth of data including evidence pertaining to ongoing investigations. They were unable to recover when backup procedures overwrote their existing good unencrypted backup with the now infected backup. This could have been avoided with multiple version, detached backup

Ransomware almost doubled in 2017, increase of 90%

One Third of IT Managers have lost data while migrating between devices or upgrading operating systems. Knoll Ontrak found that some of the top reasons was that their backup wasn't current or operating correctly

57% of IT Managers have a backup solution in plance, 75% of them were not able to restore all of their lost data.

Over half of consumers and businesses reported data loss even when a backup system was in place

Prior to a ransomware attack 4 out of 5 organizations are confident backup can provide them with complete recovery but less than half of ransomware victims fully recover their data...even with a backup

Only 6% of laptops are backed up

YOUR ONLY AS GOOD AS YOUR LAST TESTED SECURE BACKUP!!!!

Sources

https://money.cnn.com/2017/07/27/technology/business/ransomware-malwarebytes/index.html
http://bsf.co.za/the-global-cost-of-data-loss/
https://www.bostoncomputing.net/consultation/databackup/statistics/
https://clutch.co/cloud/resources/world-backup-day-2017
https://itnow.net/backup-stats-that-might-shock-you/
https://blog.malwarebytes.com/malwarebytes-news/2018/01/presenting-malwarebytes-labs-2017-state-of-malware-report/
https://blog.storagecraft.com/business-continuity-statistics-tech/
https://iosafe.com/industry-stats
https://www.datto.com/resources/ch-ransomware-survey-17
http://invenioit.com/continuity/2017-disaster-recovery-statistics/
https://www.wfaa.com/article/news/local/cockrell-hill-police-lose-years-worth-of-evidence-in-ransom-hacking/392673232
https://www.marinij.com/2016/09/29/marin-patients-medical-data-lost-after-cyber-attack/
https://www.ontrack.com/resources/press/details/63920/kroll-ontrack-research-one-third-of-companies/