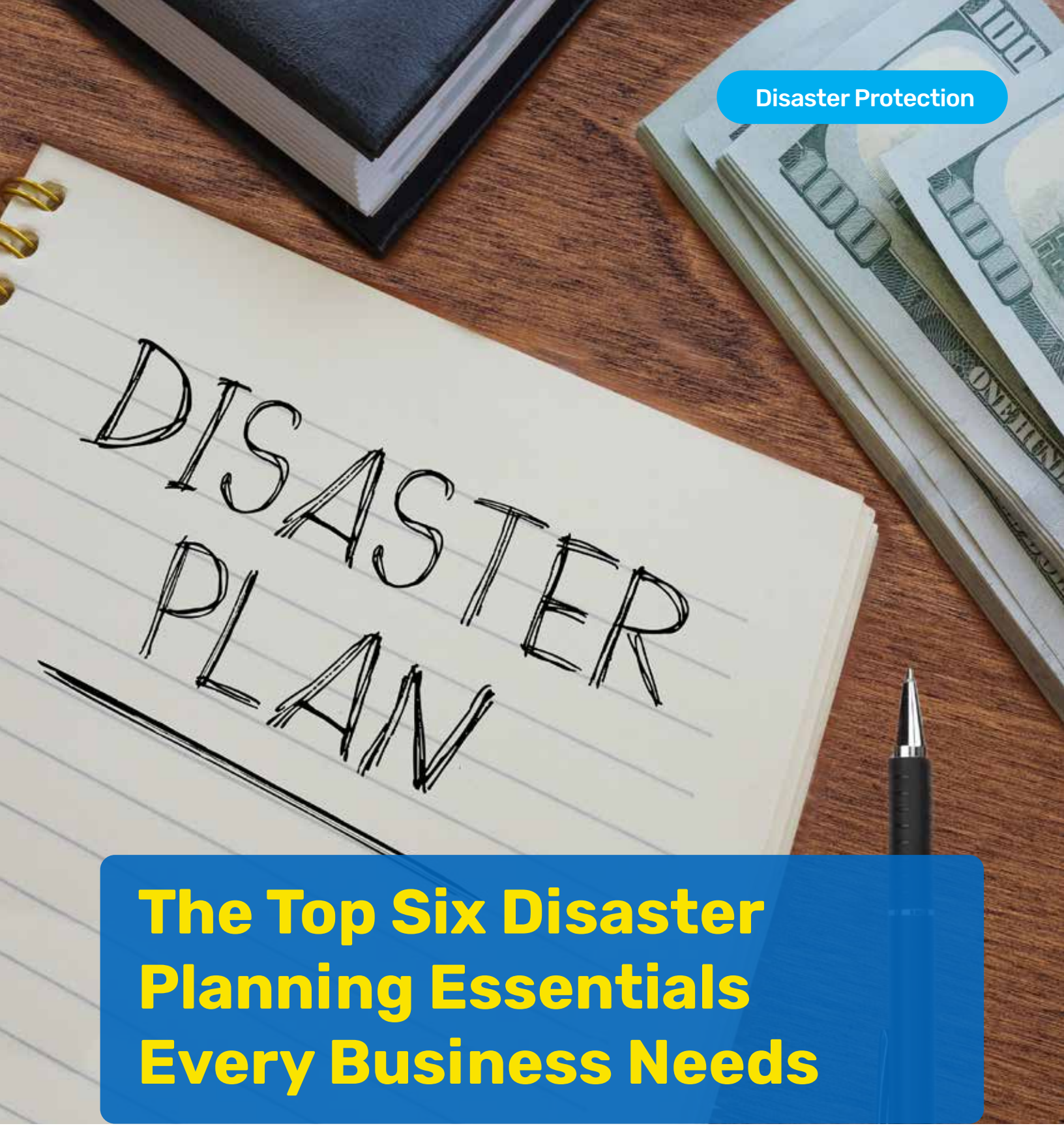


Disaster Protection

The Top Six Disaster Planning Essentials Every Business Needs

Reliable Resistant Secure

BULLET PROOF TECH GUIDES

Insider Tips To Make Your Business Run Faster, Easier, and More Profitably.

95% of companies rely on digital information and technology to serve customers and operate their business.

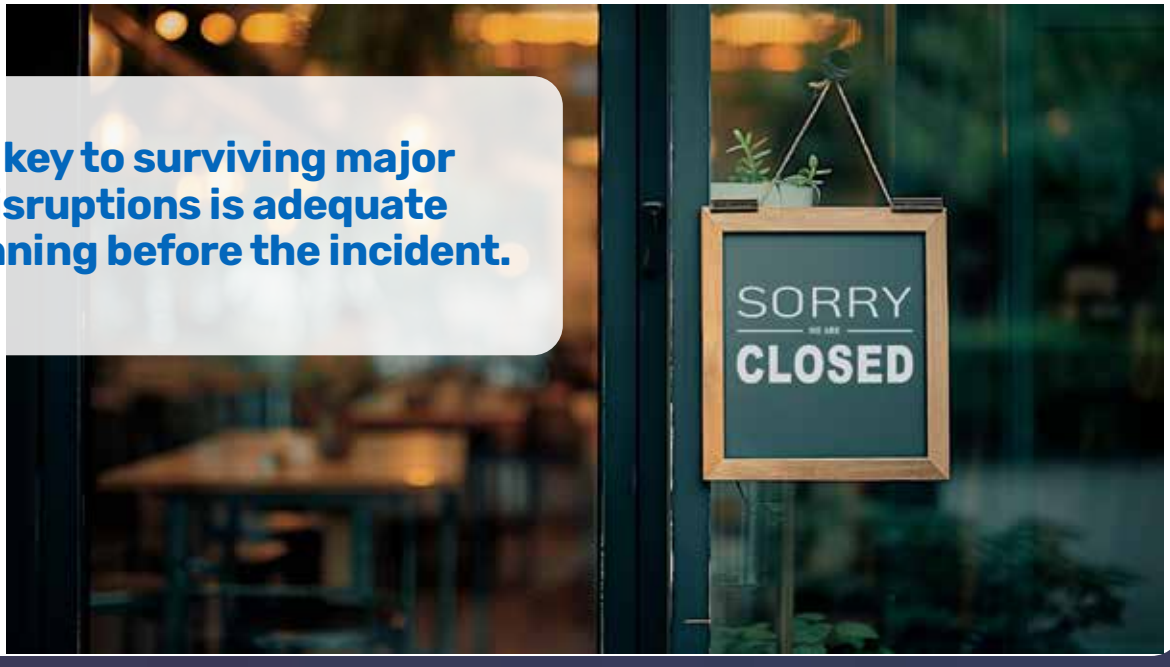
That's why it's no longer "nice" to have a disaster recovery plan for your business – it's an outright necessity to protect your business when (not if) you have a technology disaster.

What is a disaster recovery plan for a small business?

In its simplest form, a Disaster Recovery Plan is a written plan designed to provide direction, calmness, and confidence in a time of chaos. It gives the steps to take after a disruption, from who to contact (insurance, IT professional, attorney, etc.) to how to recover systems.

No matter the size, every business should have a disaster recovery plan in place. With even a simple, concise plan, if an unexpected disruption occurs, the business can minimize operational downtime and significantly reduce the risk of financial losses and, at worst, permanent closure.

The key to surviving major IT disruptions is adequate planning before the incident.

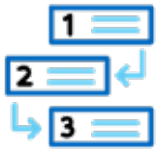


The National Institute of Standards and Technology (NIST)

sets the government and private sector's technology guidelines and base standards. They have a very long (25 pages) and geek/tech speak-filled Disaster and Planning basic template. For most small to mid-size businesses, attempting to use the NIST template typically results in frustration and scrapping the entire idea.

This guide uses the NIST template as its backbone (foundation). It provides an easy-to-understand starting point for your Disaster Recovery planning concerning your technology infrastructure (your computers, data, and network). We cover the basics that every business should have in place to protect against IT disasters of any kind. What matters most is protecting your business and being able to recover from an IT disaster, whether big or small.

Why Your Business Needs a Disaster Recovery Plan



46% of businesses have no documented disaster recovery plan. (IBM & Computing Research Report)

Among companies with a plan, 27% never test any protocols or systems written in the plan. (IBM & Computing Research Report)

40% of small businesses fail to reopen following a disaster. (FEMA)

90% of smaller companies fail within a year if they can't resume operations within 5 days after experiencing a disaster. (FEMA)

60% of organizations experienced at least one outage over the past three years. (Uptime Institute Report)

Creating an Effective Disaster Recovery Plan

Whether you use the NIST template or this scaled-back framework, creating an honest/reliable disaster plan related to your technology relies on an accurate understanding of your company's risks.

An IT-specific risk assessment is usually completed to identify the most likely threats and their impact on the business.

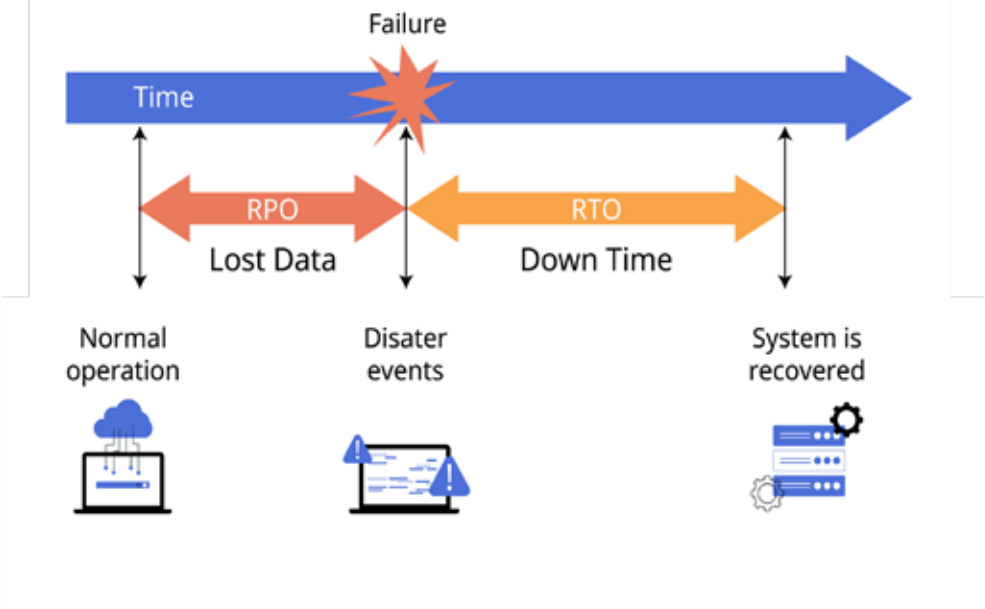
A primary component of an IT risk assessment is determining how quickly your systems should be recovered to prevent the negative consequences of a prolonged outage. Basically, how long are you comfortable with your business being down? Is it a few hours, a day, or longer? And will the practices and tools you have in place now meet your risk tolerance level?

There are two core standard objectives:

Recovery time objective (RTO): The desired maximum amount of time that the recovery process should take. This can be applied to specific systems or events, such as data loss, network outages, website outages, and so on.

Recovery point objective (RPO): The desired maximum age of the most recent backup. This objective sets a limit for the age of backups (as well as goals for backup frequency), helping to minimize the amount of data loss when a backup needs to be restored.

This assessment also covers several core areas: network security, hardware and software health, compliance and risk management, and operational efficiency.



A few examples of technical items in an IT-specific risk assessment would be:

- What security solutions are in place to prevent disruptions from malware, cyberattack, data theft, etc.?
- How are network/firewall configurations set up to block dangerous incoming/outgoing traffic?
- Are there access control/permissions to restrict users from accessing sensitive file directories?
- Is load balancing being utilized to prevent network slowdown and server crashes?
- Is server maintenance scheduled and hardware replacement planned to prevent unexpected failure?
- What current applications are in the cloud, and what are their security and data backup policies?
- Are there employee cybersecurity training programs in place?

While you may be able to answer some technical questions, we highly recommend you engage with an IT professional to evaluate your current environment and complete a risk assessment for your business.

The Anatomy of a Simplified Technology Disaster Recovery Plan

1. **Key Contacts & Other Important Information:** Insurance contacts, IT contacts, etc.
2. **Incident Recovery Procedures:** Detailed steps for recovering from specific incidents.
3. **Systems:** Data backup and other IT systems that support the recovery process.
4. **Testing:** How often are the various systems tested to ensure functionality.
5. **Review & Update Schedule:** How often is the plan reviewed and updated.

The Top 6 Essentials That Every Business, Regardless of Size, Should Include in Their Disaster Planning.

1 Have a Written Plan

As simple as it sounds, thinking through what needs to happen in case of IT disruptions is something few business owners do. It's critical to be organized, have a strategy, and have all your key information readily available in one place. Minimizing downtime and financial losses after a disaster may depend on your ability to act swiftly and decisively.

At a minimum, the plan should contain contact information for your IT Provider (if not using a full-time in-house staff member), your insurance company contact information, and your policy details. Other items typically included are details on the most critical data and systems and a step-by-step process of how those systems will be brought back online.

Most of this information can be gathered and put together by a staff member and your IT provider, leaving you to review and add details and feedback.

Here are a few overlooked items your Disaster Recovery plan should also include:

- A "Break The Glass" document of critical websites, passwords, and other information held only by key team members and executives that are critical for running the business. If something should happen, you want to be able to keep the business running.
- A telecommunications recovery plan that would deal with a situation where all phone lines are down, or your building is inaccessible.
- A list of key vendors and their contact information. You should also have emergency contact information for each employee in case of a major disaster where you cannot access your office, and you must contact them at their home.

2 Think Of Business Continuity for Various "Likely" Scenarios.

When it comes to technology, there isn't just one thing that can cause a disruption or qualify as a disaster. There are many.

Here are a few examples to consider for business continuity planning:

- Ransomware & malware that disables or destroys data
- Phishing attack that allows hackers access to banking or credit cards
- Data loss caused by accidental or malicious deletion
- Cloud Provider and other Utility company issues that you can't control
- Network outages that block internet, communication, and server access
- Hardware failure that destroys or prevents access to data
- Fire or flooding that destroys infrastructure and forces relocation

Most business owners have the mindset that "those things won't happen to me" and that the chances are "so small" that they don't plan for anything. This mindset is the worst position to be in when a disaster or disruption does happen.

Each of these real-life scenarios can pose enormous challenges for any business. Another huge mistake business owners make is thinking that having a backup copy of their data will enable them to return to business quickly, which may not be the case, depending on the disruption and your cyber liability insurance.

We often see business owners shocked to learn that if they have a cyber incident, their insurance company will NOT let them do anything until the insurance providers' "forensic auditors" have completed a review, which could take days to weeks to get scheduled.

An additional business continuity recommendation: if you have a computer used for business-critical functions or an in-house server, consider having an

"image" of that computer or server and a backup of the data.

"Imagining" is simply a process of making an exact copy of the computer or server and everything on it. When disaster strikes, that "image" can be directly copied to another device, saving enormous time, money, and frustration in getting back up and running. Best of all, you don't have to worry about losing your preferences, configurations, or favorites.

A small amount of pre-planning can translate into tremendous savings and less stress.

3 Follow the 3-2-1 Rule for your backups.

The 3-2-1 Backup Rule is a simple, effective strategy for keeping your data safe. It advises keeping three copies of your data on two different media with one copy offsite.

The process looks like this:

- **Three copies of your data:** Your original in-use data and two more copies are kept elsewhere.
- **On two different media:** You should store your data on two different forms of media, such as an external hard drive, another computer, and/or somewhere in the "cloud."
- **One copy offsite:** You should keep one copy of your data offsite in a remote location, ideally more than a few miles away from your other two copies.

The rise in ransomware attacks, where cybercriminals target networked machines and intentionally hunt down and destroy backups, is a growing problem.

Keeping a copy of your backups completely offline is necessary in today's digital landscape.

There are various methods for backing up data, each with its own pros and cons. These include:

Full backups: Making exact copies of all your data at once.

Incremental backups: Only backing up the data that has changed since the last backup, reducing storage space and time.

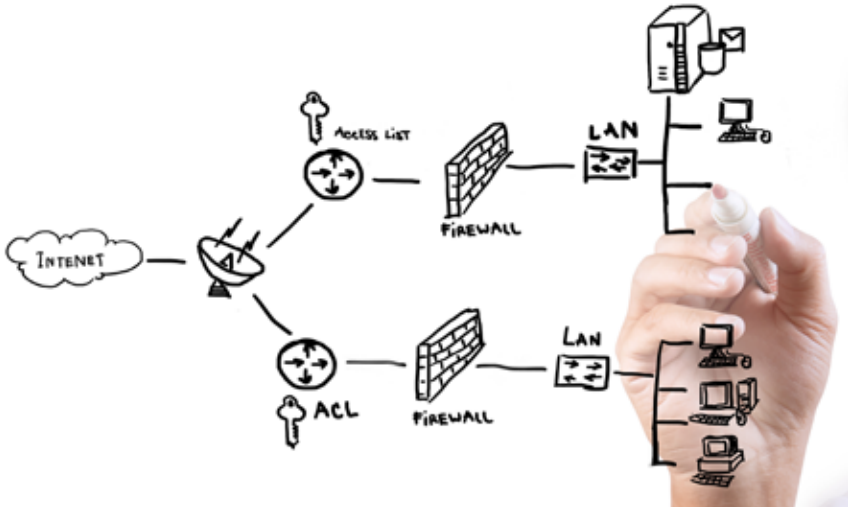
Cloud backups: Storing your data securely on remote servers accessed via the internet.

On-site backups: Keeping backups locally, such as on external hard drives or a dedicated backup device (yes these are still used today).

Hybrid backups: Combining on-site and cloud backups for added redundancy.

Following the 3-2-1 rule helps your business avoid a single point of failure vulnerable to **human error, hard drive crashes, theft, natural disasters, or ransomware.**

4 Network documentation.



Network documentation is simply the software (programs), data, and hardware you have in your company's network.

In the event of a technical issue, if you don't have all the software disks, installation codes, licenses, or user names/passwords, it could take days to reinstate your applications. Even if you have a good copy of your data from a backup, the data is useless without the applications.

Another vital reason to have this information in one place is should disaster strike; you have all the required information for insurance claims of what you lost. Keep a printed copy of this documentation with your disaster recovery plan.

5 If using cloud programs/services, have a backup plan and include it in your planning.

A massive amount of the technology companies rely on lives in the cloud.

Applications, services, and files now exist in vast data centers managed by providers like Microsoft, Intuit, Amazon, and Google. This shift has brought significant benefits: streamlined collaboration and the ability to work from almost anywhere with an internet connection.

But what happens when the services your business relies on experience outages or your internet connection goes down? Microsoft has had multiple disruptions this year alone, leaving many companies scrambling to stay productive and costing them millions of dollars in revenue.

A best practice is every important cloud application in your business should have an alternate option or another way to conduct business. If you are in the medical industry, this planning is critical for your business and patients! Several local doctors, clinics, and dentist offices have closed due to their patient software vendors experiencing issues.

Key steps for your downtime plan:

- **Enable offline access:** When available, install the local apps on all necessary devices before a disaster or outage strikes.
- **Use tools like OneDrive, Dropbox, or an onsite server:** These tools help ensure the availability of local copies of important files. When service is restored, confirm that all data has been synced.
- **Identify offline tasks:** Train employees to recognize which work can be done locally on their computers without internet access (editing documents, data entry, or organizing files).

Your business may want to consider a hybrid approach where certain services remain onsite while others reside in the cloud, which offers a safety net against unexpected disruptions.

Planning for cloud provider outages may not be exciting, but it's necessary. Having a clear plan ensures your team can adapt quickly and avoid frustration when services go down.

Three Myths That Can Damage or Destroy Your Business

"We're too small for a Disaster Plan."
Disasters don't discriminate. Cybercriminals often target small businesses because small businesses typically spend less money on security and backups. Being unprepared leaves your business with weaker defenses and vulnerable to a preventable disaster.

"It's too expensive."
Unlike five or ten years ago, there are many backup solutions available. The variety of options has made recovery affordable for businesses of all sizes. Depending on your business size and amount of data, some options start at $25.00 per month.

"We've never had an issue before, and we've got everything in the cloud, so we are safe."
Complacency is a trap. Even the most secure systems like Microsoft 365 and Google Documents have had outages for extended periods. Don't trust your business's operability to one of the big "cloud" providers.
Have a tested recovery plan.

6 Test your plan – especially your backups!

If you've taken the time to create a disaster recovery plan, you will want to test it when it's not needed.

Call the numbers listed for your insurance carrier. You would be surprised how often phone numbers and claims processes change.

Ensure that your backups are working and your data is viable and not corrupt.

The worst time to find out that your backup wasn't working is when you need it, or as the saying goes, the worst time to test your parachute is after you've jumped out of the plane.

Why Your Business Needs to Test Your Data Backups

Over 40% of businesses never test their backups. (Gartner)

58% of companies with backups find they don't work when needed. (Gartner)

60% of businesses that lose their data shut down within six months. (National Archives & Records)

Over 50% of businesses experience a yearly data loss event due to accidental deletion, system crashes, or cyberattacks. (Verizon Data Breach Investigation Report)

Regular backup testing helps you uncover any issues or weaknesses in your backup system before disaster strikes, giving you the opportunity to address them proactively.

Not all backups are created equal.

Sometimes, files may fail to back up properly, or crucial data may be inadvertently excluded from the backup process. By testing your backups regularly, you can verify the integrity and completeness of your data, making sure that everything you need is safely stored and accessible when you need it most.

Depending on your business and industry, weekly, monthly, or quarterly are general best practices.

And there are a few different methods for testing backups:

File restoration test

This involves randomly selecting files from your backups and attempting to restore them to their original location. This helps verify that individual files can be recovered successfully from the backup.

System recovery test

In this test, you simulate a complete system failure and attempt to restore your entire system from backup. This comprehensive test verifies that your backup system can successfully recover your entire infrastructure in the event of a catastrophic failure.

Validation checks

Regularly perform validation checks on your backup data to ensure its integrity and completeness. This might involve using something called checksums or hash values (which verify that data is complete and hasn't been tampered with) to check the integrity of backup files.

Downtime Isn't Just an Operational Hiccup - It's a Business Nightmare

Disaster recovery planning is not just about surviving an incident but about thriving in its aftermath.

Companies with a strong disaster strategy outperform competitors because they are prepared and can minimize disruption when disaster strikes.

Now that we've covered the six essentials to include in your disaster planning let's cover the four most likely IT disasters most businesses face. Each of these IT disasters has its own set of challenges and impacts. While these are the most prevalent types of disruptions/disasters, you may need to plan for additional types depending on your business's industry and unique characteristics.

Determining your business's specific needs is an area where an IT Professional can provide invaluable assistance.

Ransomware

Ransomware attacks are driven by deliberate and malicious intent. This attack disrupts normal operations and is designed to exploit the company by locking you out of your devices/network and demanding payment (or a ransom) for a decryption key that will restore access to your data.

The primary objective of this plan is to restore data as quickly as possible without paying a ransom that could cost millions. A secondary but equally important goal is to ensure that the infected device(s) and recovered data are free of the malware that infected it in the first place.

Phishing

A successful phishing attack can result in significant financial losses through unauthorized access to bank accounts and fraudulent transactions. A written plan with contact information and steps to take helps to shut down and mitigate these financial risks quickly.

Software and Hardware Failure

If your business is in a specialty industry and you use special software or hardware, this type of planning is critical for the long-term success of your company. Examples: specific computers and software that control the manufacturing of items or medical devices.

Software failure happens when a program or the operating system reaches an error point from which it cannot resume regular operation. The causes might be bugs, compatibility issues, or corrupted data. An example is the famous blue screen of death. The newest versions of Windows have been updated to a green screen of death.

Hardware failure typically occurs when servers, hard drives, firewalls, and network devices stop working. Reasons vary from wear and tear, manufacture, or environmental conditions such as overheating. Inappropriate configuration and failure to install available updates can also cause disastrous failure.

Natural Disasters

The most common are tornados, power surges, and water damage. Overall, natural disasters are less likely, but due to their unpredictability, planning for them can save your business in the event of one taking place.

This plan should include information about alternatives, workarounds, and what your staff can do in the event of one of these disasters.

Frequently Asked Questions

What is the best way to back up my data?

While many backup solutions are available, choosing the right one for your business depends on your risk comfort level and whether you are in a regulated industry. (medical, finance, law).

Overall, here are some key capabilities to look for when comparing options:

- Dedicated backup devices to process and store the backups
- Hybrid cloud backups (stored locally and in the cloud)
- Ability to perform backups frequently (every few minutes or more frequently)
- Ability to boot backups as virtual machines for instant access to protected files, apps, and operating systems
- Multiple recovery options: file-level, rollback, direct restore, etc.
- Offline/offsite backup to help protect against ransomware

If I'm using Microsoft 365 and Quickbooks Online and their data backup, why do I have to worry about data backups?

All Cloud providers adhere to the Shared Responsibility Model, including Intuit, Microsoft 365, Slack, Google Workspace, Asana, Xero, etc.

The quick summary of the Shared Responsibility Model is all cloud providers maintain the building and servers and ensure they work. They also support the internet connection that allows you to connect to them ~ and that is it.

Yes, most Cloud providers also say they can/do back up your data. However, no cloud provider, it doesn't matter if it's Intuit or Microsoft, is responsible for what data you are backing up, if it is usable (able to restore in an emergency), or how long it takes to get your data if you need it.

For 99% of cloud services, in the terms and conditions, there is a section stating that you are solely responsible for your data and hold the cloud provider harmless (which means you cannot sue) if you lose your data or if their service goes out and you can't work. You are legally bound by their terms when you click the "I agree" button.

From a business risk perspective, we recommend not relying solely on the Cloud providers' data backup.

I have cyber liability insurance – shouldn't that cover my technology disasters?

While Every carrier and policy is different, and you will want to talk to your insurance agent about your business-specific policy.

With that said, here are a few things to keep in mind regarding Cyber Insurance: premiums are increasing, certain coverages are being dropped, and it's getting harder to qualify. Some companies now exclude ransomware coverage or cover it as an add-on "rider" policy. Most insurance carriers are also basing your premiums on the security protocols your business has in place ~ this would include having a disaster recovery plan.

The biggest thing to understand about your cyber liability insurance is that the devil is in the details ~ make sure you know the fine print.

How to protect your business in today's digital world

Keeping up to date with the latest trends, threats, and best practices in online security is essential for maintaining effective defenses against cyber threats.

But it's a full-time job. Which is another reason you should consider partnering with an IT support provider (like us) to keep you secure and ahead of the curve.

We subscribe to industry publications, newsletters, and blogs to stay informed about emerging threats, new attack techniques, and security vulnerabilities. We do it so you don't have to.

And we keep our clients safe by handling the security and technology that runs their business, so they don't have to think about it.

Want an easy stress free way to protect your business? Get in touch.

CALL: 615-826-0017
EMAIL: info@gsgcomputers.com
WEBSITE: www.gsgcomputers.com

GSG Computers
Bullet Proof Your Technology